USERS

OPTIMICE RECURSOS Y REDUZCA COSTOS DE EQUIPAMIENTO Y SOFTWARE

ADMINISTRADOR DE SERVIDORES

HERRAMIENTAS, CONSEJOS Y PROCEDIMIENTOS PARA EL PROFESIONAL



- INSTALACIÓN, CONTROL, MONITOREO Y PUESTA A PUNTO DE SERVIDORES
- SEGURIDAD CORPORATIVA: POLÍTICAS Y NORMAS
- TÉCNICAS AVANZADAS DE VIRTUALIZACIÓN
- REPORTES E INFORMES DE INFRAESTRUCTURA
- ADEMÁS: SCCM, VMWARE, CLOUD COMPUTING, INVESTIGACIÓN EN IT



ADMINISTRADOR DE SERVIDORES

HERRAMIENTAS, CONSEJOS Y PROCEDIMIENTOS DE LA ACTIVIDAD DIARIA

por Marchionni, Enzo Augusto

RedUSERS



TÍTULO: Administrador de servidores

AUTOR: Enzo Augusto Marchionni

COLECCIÓN: Manuales USERS

FORMATO: 17 x 24 cm

PÁGINAS: 352

ISBN 978-987-1773-19-0

Marchionni, Enzo Augusto
Administrador de servidores. - 1a ed. - Buenos Aires : Fox Andina; Banfield - Lomas de Zamora: Gradi, 2011.
352 p. ; 24x17 cm. - (Manual users; 210)

ISBN 978-987-1773-19-0

1. Informática. I. Título.

CDD 005.3

Marchionni, Enzo Augusto



Es Analista Universitario en Sistemas de Información y estudiante de Ingeniería en Sistemas de la Universidad Tecnológica Nacional. Se especializó en VMware y SCCM a lo largo de su carrera. Trabaja actualmente en HP como tecnólogo de plataforma en Tenaris. Mantiene su blog **www.infosobresistemas.blogspot.com** y escribe para esta editorial. Hasta el año 2010 administró los servidores internos a la compañía Global Crossing. Durante 2009 coordinó la comisión de tecnología del grupo La Plata Valley, donde logró acercar a su ciudad natal a representantes de Microsoft, Globant y Google. De 2005 a 2007 fue desarrollador de los sistemas informáticos de CUCAIBA. Desde el año 2001 hasta la actualidad se dedica a negocios de tecnología, consultoría, redes físicas y sociales, sistemas y venta de equipos. Mantiene la web de la fábrica de muebles de la familia **www.cmarchionni.com** y ha generado a lo largo de su carrera varios sistemas informáticos.

Dedicatoria

A Liliana Mabel Montes de Oca y Cesar Alberto Marchionni, mis padres.

Agradecimientos

A los que me enseñaron, compañeros de trabajos y amigos.
A mi actual compañera de la vida, Valeria Giselle Gempel Miri, y flía.

PRÓLOGO

La administración de servidores no es una tarea fácil, y aunque es una actividad que cada día adquiere mayor importancia, no maneja conceptos que se enseñen en forma habitual. De manera general asociamos el concepto de sistemas con el desarrollo de aplicaciones informáticas, pero debemos tener en cuenta que la administración de servidores es una tarea mucho más compleja, ya que no sólo se ocupa de instalar hardware y controlar los sistemas existentes, sino que también debe lidiar con la responsabilidad de mantener el grupo de sistemas funcionando y solucionar las dificultades que pudieran presentarse. En este sentido, la administración de servidores tiene una visión más amplia de toda la empresa y también de la tecnología que se maneja en ella. Además, gracias al desarrollo de aplicaciones, puede automatizar ciertas actividades, controlar y obtener reportes, entre otras tareas.

En la década del 60, IBM inventaba la virtualización en los grandes servidores mainframe; desde entonces hasta ahora, han ocurrido muchos cambios. En la actualidad, la virtualización es una necesidad, una solución y también un camino a seguir por todas las empresas, ya que no sólo origina un mejor aprovechamiento del hardware, sino que genera grandes ahorros de energía y de horas de administración. Gracias a esta poderosa herramienta, podemos acercarnos a lograr la continuidad del negocio.

La administración de servidores necesita de personas responsables, analíticas, con rápidos reflejos y que sepan resolver problemas. Las empresas requieren de especialistas, y nosotros podemos llegar a ser uno de ellos. En este libro se mezcla la administración, la operación y la arquitectura de los sistemas, pero sólo depende de nosotros el camino que elijamos recorrer y hasta dónde podemos llegar.

Este libro pretende entregar una ayuda a los lectores que desean acercarse a la administración de servidores, proporcionando una visión de todas las tareas que se deben realizar. Espero que esta obra se convierta en el sendero que los ayude a transitar por el poco difundido y complejo mundo de la administración de servidores.

Suerte.

Enzo Marchionni

EL LIBRO DE UN VISTAZO

La finalidad de este libro es dar al lector una introducción al mundo de la administración de servidores corporativos. Veremos en los primeros capítulos los elementos que hay que conocer para ir adentrándonos en sus configuraciones y funcionalidades. El lector podrá tomar conocimiento de la seguridad y responsabilidad de este trabajo a medida que avanzan los capítulos. Luego, conocerá las últimas tecnologías del mercado IT a través del desarrollo de los temas de virtualización con VMware y de la administración centralizada que ofrece SCCM.

Capítulo 1

ADMINISTRACIÓN INTERNA DE UNA EMPRESA

En este capítulo conoceremos los servidores, aquellas máquinas que debemos cuidar para darle continuidad al negocio. Veremos sus características principales, los tipos y servicios necesarios para una empresa, su interconexión, el equipamiento necesario y otros elementos. Por último, una breve introducción a las responsabilidades de ser un administrador de servidores y unos consejos para las horas de trabajo.

Capítulo 2

CONFIGURACIONES DEL SERVIDOR

Aquí veremos los pasos que debemos seguir para instalar un servidor en nuestra empresa, conoceremos los directorios de dominio y aprenderemos las configuraciones básicas de la red para el servidor. Luego describiremos las aplicaciones y los servicios que se necesitan en una red corporativa y, por último, las herramientas que nos van a ayudar a controlar todos estos aspectos.

Capítulo 3

SEGURIDAD CORPORATIVA

Nos adentraremos en el campo de la seguridad aprendiendo todos sus matices. Conoceremos qué son las políticas de un dominio y el papel fundamental que juegan en nuestras tareas diarias. Luego aprenderemos cómo es el ingreso a los centros de cómputos, qué normas de seguridad internacionales nos van a ayudar en distintas tareas, y qué sistemas de antivirus y firewall son los recomendados en el mercado actual.

Capítulo 4

VIRTUALIZACIÓN DE SERVIDORES

En este capítulo aprenderemos qué es la virtualización de la mano de VMware, uno de los mayores responsables del mercado. Iremos viendo las distintas herramientas que podemos utilizar, empezando con aplicaciones sencillas de escritorio y dirigiéndonos a las aplicaciones corporativas como son los servidores ESX y Virtual Center. Para finalizar, una breve descripción de servidores prefabricados que podemos echar a andar en segundos.

Capítulo 5

ADMINISTRAR VMWARE VSPHERE

Aquí extenderemos el concepto de virtualización para entender de qué manera funciona un datacenter virtualizado. Conoceremos la herramienta principal involucrada en todo esto, llamada VMware vSphere y las grandes posibilidades de manejo de nuestro ambiente virtual que nos brinda. Describiremos sus conceptos y utilidades para luego conocer

cómo se manejan los backups en virtualización, analizando las distintas soluciones que tenemos hasta la fecha.

Capítulo 6

SYSTEM CENTER CONFIGURATION MANAGER

Con el capítulo anterior finalizamos la administración virtualizada, y pasamos aquí a ver otra gran herramienta llamada System Center Configuration Manager. Conoceremos a los integrantes de su familia y aprenderemos a instalarla. Luego detallaremos algunos aspectos importantes con respecto a los clientes que deberemos instalar en los servidores y los puntos de distribución de software y parches de seguridad.

Capítulo 7

PROGRAMAS, PARCHES E INFORMACIÓN

Aprenderemos en este capítulo por qué es tan importante contar con esta herramienta en nuestra empresa. Veremos cómo es el tratamiento de la distribución de parches y software para todos los servidores de nuestra infraestructura, y por último, conoceremos los espectaculares reportes que podemos obtener con SCCM. También, un breve detalle de la base de datos que soporta a la herramienta.

Apéndice

CÓMO EXPANDIR LA TECNOLOGÍA DE LA EMPRESA

En esta sección explicaremos de qué manera expandir la tecnología de la empresa con las últimas herramientas del mercado. Presentaremos los conceptos de la virtualización de escritorio y de cloud computing. Luego veremos algunos consejos para la hora de la investigación y una serie de sitios que nos van a ayudar en la tarea.

Servicios al lector

En este apartado final incluimos una completa guía de sitios web recomendados, donde encontraremos más información y recursos sobre la administración de servidores corporativos.



INFORMACIÓN COMPLEMENTARIA

A lo largo de este manual encontrará una serie de recuadros que le brindarán información complementaria: curiosidades, trucos, ideas y consejos sobre los temas tratados.
Cada recuadro está identificado con uno de los siguientes iconos:

 CURIOSIDADES E IDEAS

 ATENCIÓN

 DATOS ÚTILES Y NOVEDADES

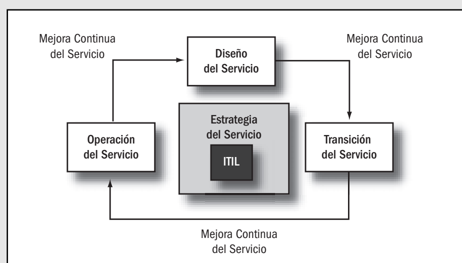
 SITIOS WEB

CONTENIDO

Conexión cruzada

Conexión derecha

Capítulo 3



Capítulo 4

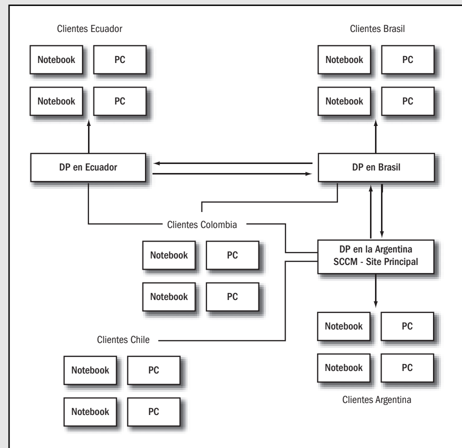


Capítulo 5

Capítulo 6

SYSTEM CENTER CONFIGURATION MANAGER





Capítulo 7

PROGRAMAS, PARCHES E INFORMACIÓN



Apéndice

CÓMO EXPANDIR LA TECNOLOGÍA DE LA EMPRESA



Servicios al lector

INTRODUCCIÓN

Ésta es una obra que pretende captar la atención de aquellas personas dedicadas a la reparación de computadoras o a la creación de redes y que deseen especializarse o comenzar a entender el mundo de la administración de servidores corporativos.
El libro comienza con un breve resumen de los conceptos básicos y, posteriormente, se enfoca en dos temas muy importantes para la administración de servidores: la virtualización y el sistema SCCM. La virtualización con VMware desbarrancó a todas las soluciones del mercado, en tanto que el sistema SCCM (System Center Configuration Manager), de la empresa Microsoft, se especializa en el manejo de información de la compañía a nivel de inventario, reportes en línea y distribución de parches y software. Ambos sistemas se encargan de generar grandes ahorros y aumentar la confiabilidad en la empresa. Es preciso saber que ambos se encuentran en constante crecimiento, por lo que será necesario contar con personal especializado en su manejo.
Debemos tener en cuenta que no hace falta ser especialista en servidores para leer este libro; para disfrutar de todo su potencial bastará con tener unos pocos conocimientos básicos en el manejo de sistemas operativos. Esta obra tiene muchas prácticas con las cuales podemos realizar las distintas tareas que se detallan y, de esta forma, tomar confianza para ejecutar ejercicios propios. El fin principal de este libro es que aprendamos a administrar la infraestructura corporativa priorizando siempre un objetivo principal: la continuidad del negocio. En este sentido SCCM y VMWARE son las herramientas principales para cumplir nuestra meta, ya que se encargan de generar grandes cambios en las empresas y en la forma de proceder de sus empleados. El área de Sistemas se transforma y se moderniza día a día, para enfocarse especialmente en las necesidades del negocio y no en los problemas.
Esperamos que el contenido volcado en esta obra le sirva al lector en la tarea de aproximarse a los servidores, para luego poder investigar nuevas tecnologías muy sobresalientes en el mercado, como herramientas de cloud computing y la virtualización de máquinas de escritorio.

Enzo Augusto Marchionni

Administración interna de una empresa

En este capítulo veremos conceptos básicos sobre redes y las diferentes categorías que existen. Haremos referencia a la infraestructura de una empresa, los servidores y las responsabilidades que se deben asumir. Conoceremos herramientas, servicios y los riesgos en la administración de servidores.

INFRAESTRUCTURA DE UNA EMPRESA

En esta sección conoceremos los componentes y equipos que soportan toda la infraestructura de una empresa y su funcionamiento. Aprenderemos a reconocerlos y a entender cuál es la función que cumplen.

Tipos de redes

Es importante saber que existen muchas formas de categorizar las redes: por sus características físicas o extensión, por sus características lógicas, diseños, fines, y otras. Según su alcance, las redes de datos pueden ser divididas en cuatro grupos principales: PAN, LAN, MAN y WAN.

REDES	ALCANCES
PAN (Personal Area Network)	Son aquellas que están a nuestro alrededor, no más allá del alcance de nuestros brazos.
LAN (Local Area Network)	Son locales para una empresa o edificio, aproximadamente de 1 km de extensión.
MAN (Metropolitan Area Network)	Se extienden hasta los confines de una ciudad, alrededor de 50 km.
WAN (Wide Area Network)	Son las más extensas; Internet es un ejemplo, y también las redes de una empresa mundial. Generarían altas pérdidas económicas si dejaran de funcionar.

Tabla 1. *Categorías de las redes según su alcance.*

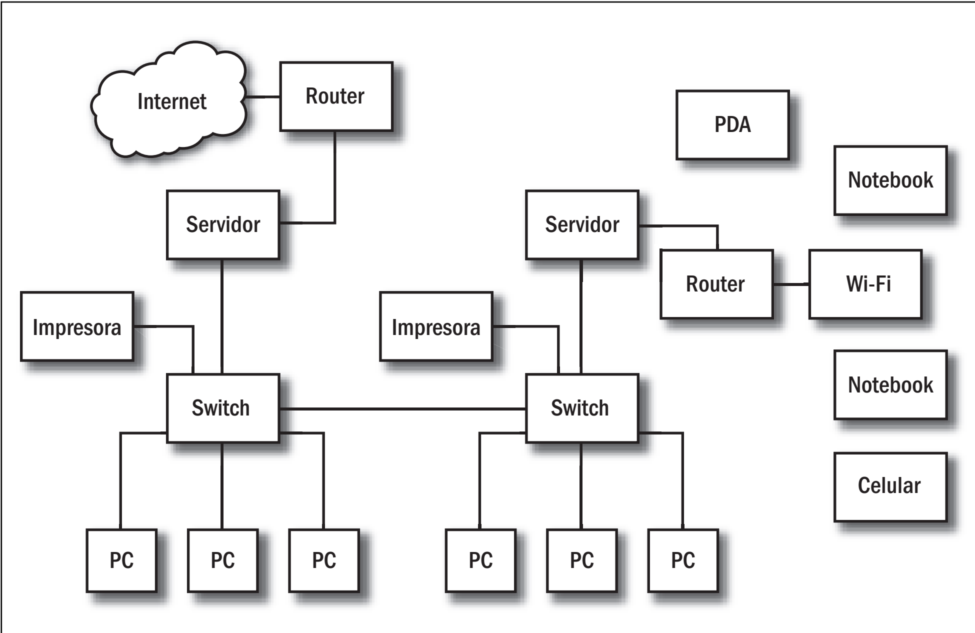


Figura 1. *Una gran red empresarial debe conectarse a Internet. En ella se observan equipos de escritorio, laptops, teléfonos, access points, servidores, routers y switches.*

Otra categorización que podemos hacer está dada por la manera en que se conectan sus componentes de hardware. Y una más se refiere al diseño de la conexión, a cómo están distribuidos los elementos en el espacio. También pueden variar de acuerdo con el software empleado, si son redes punto a punto o privadas, etc. Una última categorización las divide según sus fines.

CATEGORIZACIÓN	DESCRIPCIÓN
Hardware de conexión	Cableadas, inalámbricas, infrarrojas, satelitales
Topología	Estrella, anillo, malla, mixta, árbol
Tecnología de software	P2P, FTP, sociales, privadas, públicas
Función o fin	Universitarias, militares, científicas, etc.

***Tabla 2.** Otras categorizaciones de las redes.*

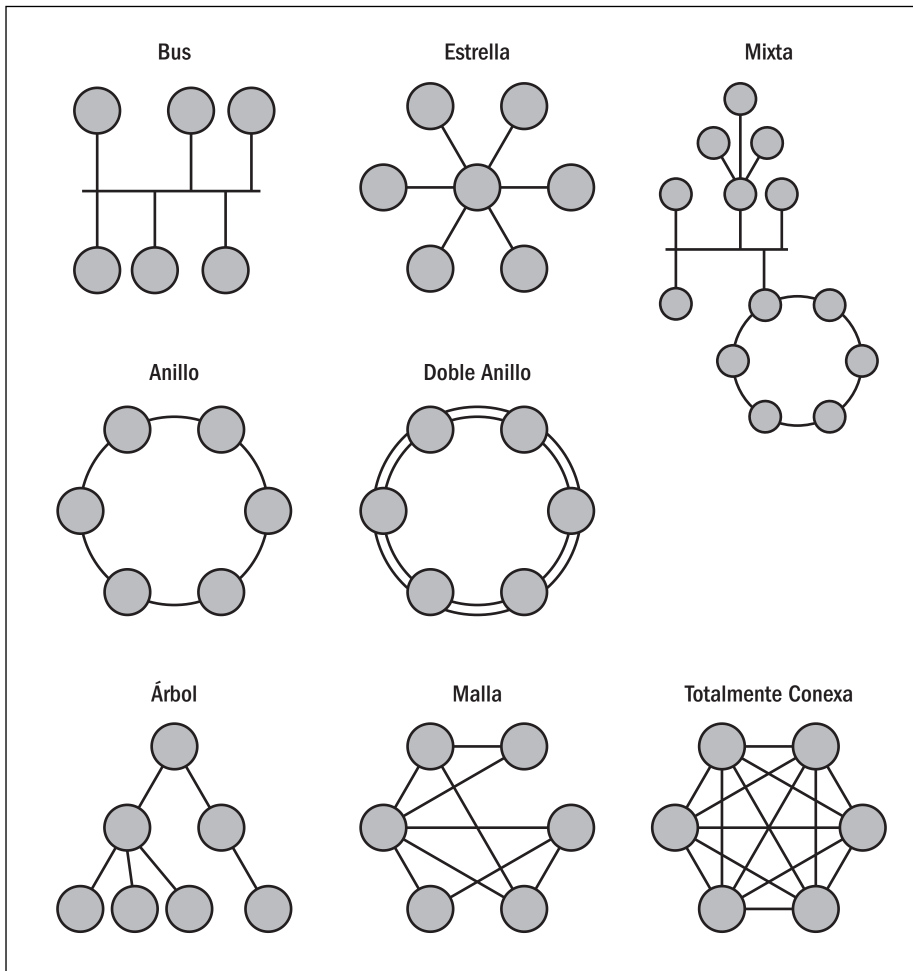


***Figura 2.** Distintas conexiones posibles entre varios equipos de la red. La más utilizada es la topología estrella.*

Una importante categoría es la de las redes privadas, de las cuales hay muchas a nivel nacional, internacional e intercontinental. Pueden estar interconectadas a Internet o no, y pertenecen exclusivamente a organizaciones e instituciones. Por ejemplo:

- **ARPANET** (*Advanced Research Projects Agency Network*): fue la primera red militar, y es reconocida porque fue la espina dorsal de Internet. Comunicaba los centros de investigación con las bases militares y las casas de gobierno.
- **NSFNET** (*National Science Foundation Network*): es una red constituida por tres niveles. En el nivel 1 se encuentra una red troncal que comunica el departamento de administración con el de operación y con redes intercontinentales. El nivel 2 está constituido por una red que comunica redes regionales, basadas en disciplinas y redes de consorcios. El nivel 3 es una red de campus, de universidades y de comercios.
- **EBONE** (*Pan-European Multi-Protocol Backbone*): cumple el mismo papel que la NSFNET, pero en las redes de Europa.
- **EARN** (*European Academic Research Network*): es una gran red que da servicios a instituciones académicas y de investigación en Europa, África y Oriente Medio.
- **ARIU** (*Asociación Redes de Interconexión Universitaria*): red argentina organizada por las universidades nacionales e institutos universitarios integrantes del CIN (Consejo Interuniversitario Nacional).

Equipamiento de una red

La red permite enviar mensajes, y en el proceso de comunicación se involucran siempre estos tres actores: un **emisor**, un **medio** y un **receptor**. El emisor es el objeto que genera el mensaje, por ejemplo, una PC de escritorio, un micrófono o una estación de radio. El medio es el camino que debe atravesar el mensaje entre el emisor y el receptor. Por último, debemos tener en cuenta que el receptor es el que entiende y recibe el mensaje originado por el emisor.

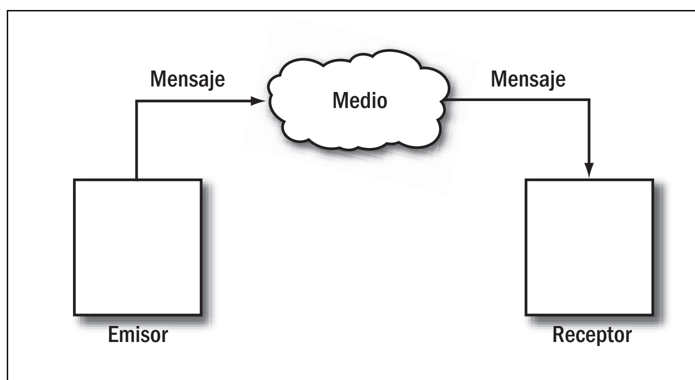


Figura 3. *Diagrama en bloques de un sistema de comunicaciones básico. El medio generaliza todos los elementos por donde puede pasar el mensaje que se va a enviar.*

Los dispositivos en la red pueden tomar el rol de cualquiera de los tres actores antes mencionados. Por ejemplo, éste sería el caso de la comunicación entre dos routers. Uno puede actuar como emisor del mensaje, y el otro, como receptor. Si analizamos una comunicación entre dos servidores, el router actúa como parte del medio por donde pasa el mensaje. A continuación, haremos una breve descripción de varios dispositivos que podemos encontrar en una red.

- **Router**: se trata de un dispositivo que dirige los paquetes de una red hacia otra. Es usado como puente para conectar redes.



***Figura 4.** Un router en cada extremo de las redes por conectar dirige el tráfico desde y hacia él.*

- **Switch**: se encarga de aumentar la capacidad de conexión en una red y direcciona los paquetes a los clientes que los solicitan.



***Figura 5.** Los switches se colocan en los racks; podemos distinguir rápidamente un switch hogareño por la cantidad de bocas que posee.*

- **Firewall**: este importante dispositivo se encarga de aplicar ciertas reglas de navegación y filtrado en las redes, que hayamos definido con anticipación; permite y deniega el acceso a ciertos puertos y protocolos.

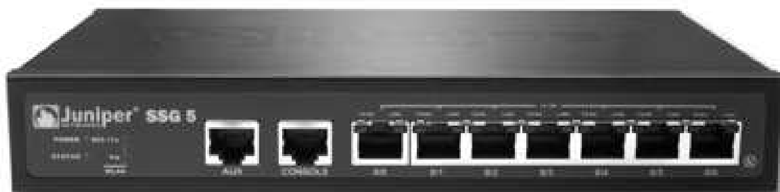


Figura 6. *Los firewalls se colocan en el extremo de la red de cara a Internet. Actúan como puerta de entrada a nuestra empresa.*

- **Sniffer**: permite analizar las tramas de la red buscando anomalías, intromisiones inapropiadas y agujeros de seguridad.



Figura 7. *Un sniffer QNAP es un ejemplo de este tipo de equipos que se conectan a la red y filtran todos los paquetes que circulan por ella.*

- **Access point**: es un punto de publicación y acceso mediante conexiones wireless.



Figura 8. *Los access points dan flexibilidad y extensión a la red. Nos permiten trabajar exentos de cables, con mayor comodidad.*

- **Rack**: es un armario metálico donde van fijados los servidores, routers, switches y pacheras. Su principal función es permitirnos organizar el espacio, y establecer una línea de enfriamiento y de conexión ordenada.



Figura 9. *En cada ubicación podemos colocar un servidor, un switch, un router o cualquier otro dispositivo. Los servidores tienen correderas para facilitar el acceso.*

- **Pachera**: permite ordenar las conexiones entre los racks, los switches y los routers. Debemos tener en cuenta que al igual que los racks, son elementos que pertenecen al medio y no actúan nunca como emisor o receptor.



MODELOS DE BASE DE DATOS

Existen bases de datos organizadas jerárquicamente, bases de red organizadas como un grafo, bases transaccionales que envían y reciben información a grandes velocidades, bases relacionales que se conforman con relaciones de datos, bases orientadas a objetos que utilizan ese paradigma para organizarse, y bases distribuidas por varios lugares al mismo tiempo.

Herramientas necesarias para un administrador

Para configurar cada uno de los equipos antes descriptos, necesitamos herramientas, como pinzas para armar cables, destornilladores, pacheras, terminales, cables de distintos tipos y longitud, y también, analizadores de conectividad y consolas seriales para realizar la configuración.



***Figura 10.** Algunas herramientas básicas para el administrador de redes en una empresa: pinza para armar cables, medidores de fibra óptica, alicate, etc.*

Un elemento importante son los cables de red. Podemos armarlos cruzados o derechos. Se distinguen por la ubicación de los cables en las fichas **RJ45**.

CONSOLAS SERIALES

Las consolas seriales se encargan de realizar la administración de equipos del tipo firewall, switch o router de manera segura. La computadora se conecta al puerto serial; hay que hacerlo desde el equipo, no es posible en forma remota. Podemos habilitar otras alternativas de conexión, crear usuarios y volver el equipo a su estado original de fabricación.

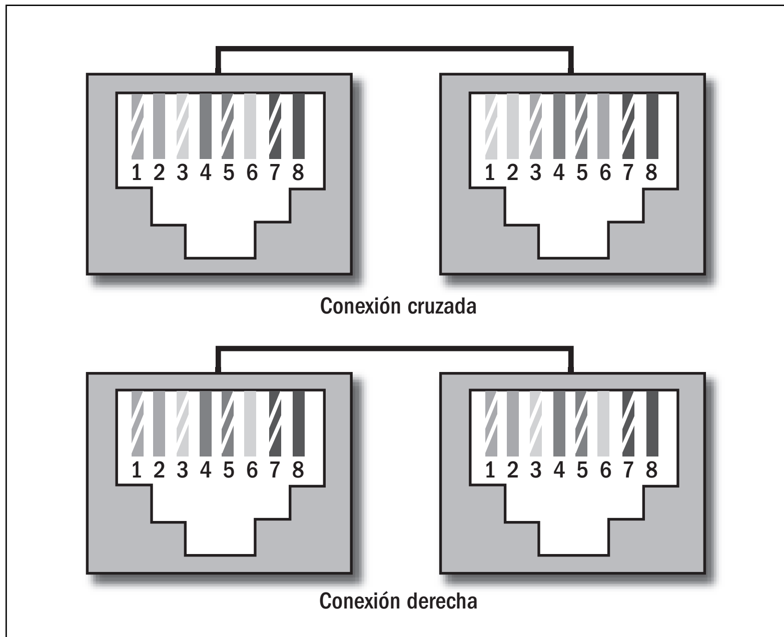
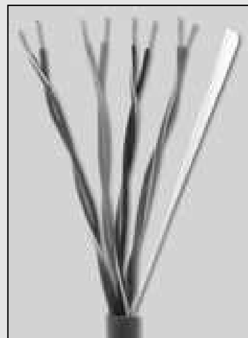


***Figura 11.** Los cables cruzados tienen diferencias entre los pares verdes y los naranjas. En los derechos, se conectan de igual forma en ambos lados.*

De forma derecha, los cables se conectan igual en las dos fichas; en caso contrario, se intercambian algunos de ellos. El cable cruzado se utiliza para una red de máquina a máquina, mientras que el derecho va conectado a un switch o hub que funciona como intermediario con las otras máquinas.

■ Armado de un cable UTP de red — PASO A PASO

1 Una vez que haya elegido la forma de armar el cable, busque una pinza de red y un cable UTP. Retire el cobertor exterior y deje libre alrededor de 15 cm. Luego, haga un corte transversal para que queden todos al mismo nivel.



▶

2 Introduzca los cables en la ficha RJ45 en forma cuidadosa. Luego coloque la ficha dentro de la pinza. Cierre la pinza para que los conectores de la ficha atraviesen cada cable. Compruebe que no quede ningún cable interno sin hacer contacto.



3 Verifique el buen funcionamiento utilizando una herramienta llamada **testeador de cables**. Enchufe los dos extremos a la herramienta, y las luces le indicarán la transmisión por cada cable. Si no posee esta herramienta, puede hacer el chequeo con un tester común verificando la conectividad en cada conector.



VIRTUAL LABS MICROSOFT

Microsoft permite entrar en su sitio web **http://technet.microsoft.com** y, de manera online, experimentar con alguno de sus servidores virtuales. Debemos ir hasta el lugar de aprendizaje y allí buscar las prácticas virtuales, que sirven para probar o conocer alguna aplicación nueva. Allí se brinda un servidor virtual ya instalado y configurado para tales fines.

SERVIDORES EN UNA RED CORPORATIVA

Luego de conocer un poco más sobre la infraestructura de una red empresarial, analizaremos cuál es el elemento responsable de dar los servicios en la red. Veremos qué es un servidor, qué funciones puede cumplir y cuán importante es en nuestro trabajo diario. También aprenderemos sobre otros elementos que podemos llegar a encontrar.

¿Qué son los servidores?

Un servidor puede encontrarse en un típico local que ofrece el uso de computadoras a sus clientes. La máquina que tiene el cajero da un servicio; es un servidor, encargado de habilitar o deshabilitar una PC para que pueda ser usada para navegar o jugar. Si deja de funcionar, el negocio no factura, y ninguna de las máquinas cliente podría ser utilizada. Los servidores son equipos informáticos que brindan un servicio en la red. Dan información a otros servidores y a los usuarios. Son equipos de mayores prestaciones y dimensiones que una PC de escritorio. Una computadora común tiene un solo procesador, a veces de varios núcleos, pero uno solo. Incluye un disco rígido para el almacenamiento de datos con una capacidad de 250 GB a 300 GB, en tanto que la memoria RAM suele ser de 2 a 16 GB. Un servidor, en cambio, suele ser más potente. Puede tener varios procesadores con varios núcleos cada uno; incluye grandes cantidades de memoria RAM, entre 16 GB a 1 TB, o más; mientras que el espacio de almacenamiento ya no se limita a un disco duro, sino que puede haber varios de ellos, con capacidad del orden del TB. Debido a sus capacidades, un servidor puede dar un solo servicio o más de uno.

EJEMPLOS EN EQUIPOS DELL	SERVIDOR POWEREDGE R910	PC DE ESCRITORIO OPTIPLEX 960
Microprocesador	Eight-Core Intel Xeon 7500 and 6500 Series, hasta 24 MB de caché L3	Intel Core2 Quad Processor, hasta 12 MB de caché L2
Disco duro	Hasta 9 TB SSD y SAS	Hasta 320 GB SATA II
Memoria RAM	Hasta 1 TB, ECC DDR3, 1066 MHz	Hasta 16 GB, DDR2 SDRAM, 800 MHz
Placa gráfica	Matrox® G200eW w/ 8 MB	512 MB NVIDIA NVS 420 Quad Monitor

***Tabla 3.** Comparación entre las características de una PC de escritorio y un servidor.*

TIPOS DE CLOUD COMPUTING

Hay tres tipos de computación en la nube: SaaS, en el que una empresa mantiene y da soporte a aplicaciones que utiliza el cliente durante un tiempo determinado; IaaS, donde la empresa da servidores y equipamientos de red al cliente; y PaaS, en que la empresa brinda una plataforma completa de software y hardware para una aplicación particular.



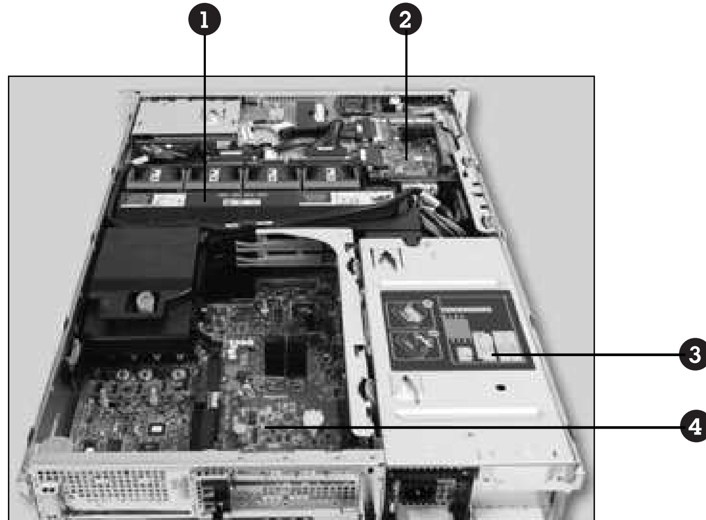
Figura 12. *Un servidor PowerEdge R910. DELL siempre se caracterizó por las buenas presentaciones de sus productos.*



Figura 13. *En esta figura podemos ver tres modelos de PC DELL OptiPlex 960; la diferencia entre ellos está dada por su tamaño y los recursos que poseen.*

Ahora que vimos bien las diferencias entre un servidor y una computadora común, podemos realizar un análisis en detalle de cómo es un servidor por dentro y qué partes de su hardware son las más importantes.

Servidor GUÍA VISUAL



1 **Refrigeración**: este sistema es muy importante, ya que si deja de funcionar, el servidor se verá en serios problemas.
2 **HDs**: aquí está el espacio reservado para los discos rígidos. Éstos se pueden sacar y volver a colocar estando el servidor encendido, sin que haya pérdida de datos; se reconstruye el disco nuevo y sigue funcionando. Esto se conoce como RAID.
3 **Fuentes**: en este lugar se ubican las fuentes de energía. Es posible apreciar el espacio para ventilación con los ventiladores propios.
4 **Placas y micro**: es la ubicación de la memoria RAM, la CPU y las placas de expansión, así como también de disipadores, cables y conectores.

Tipos de servidores

Existen distintos tipos de servidores, y pueden ser virtuales o físicos. Podemos clasificarlos según sus capacidades, fabricantes y servicios prestados. A continuación, describiremos esta última categorización:

- **Servidores de impresión**: tienen conectadas varias impresoras de red y administran las colas de impresión según la petición de sus clientes.
- **Servidores web**: este tipo de servidores se encargan de almacenar sitios en la red interna (intranet). Pueden publicar cualquier aplicación web, brindarle la seguridad correspondiente y administrarla por completo.
- **Servidores de base de datos**: lo más importante de estos servidores es la posibilidad de manejar grandes cantidades de datos y generar información. Para contener todo ese material generalmente se conectan a un storage.



***Figura 14.** Hay varias empresas que se dedican a fabricar unidades de storage. Ésta tiene capacidad para 15 unidades de disco, pero esto puede variar.*

- **Servidores de correo electrónico**: son capaces de administrar todos los correos de la empresa en un solo lugar. También trabajan con un storage, debido a la gran cantidad de datos que manejan. Allí se almacenan los correos, y se los redirecciona a clientes y servidores de seguridad, analizadores y replicadores. Algunos también brindan opciones de seguridad, como antispam, lista blanca, lista negra y antivirus.

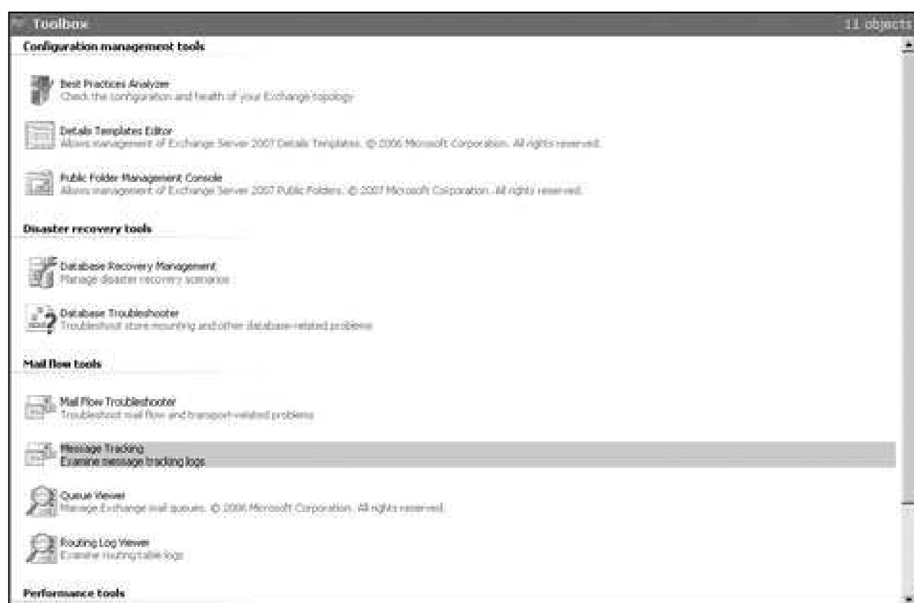


***Figura 15.** La consola de Exchange 2007, de Microsoft, dispone de varias herramientas, como búsqueda de mensajes, vista de la cola de e-mails, búsqueda de problemas, y más.*

- **Servidores de directorio**: se ocupan de almacenar los datos de todos los usuarios de la red, propiedades y características que los identifican. Veremos más sobre este tema en el **Capítulo 2**, en el apartado Directorio de dominio.
- **Servidores de comunicaciones**: brindan servicios de chat, telefonía IP, teleconferencia, video, etc. También son capaces de entregar servicios de preatendedor si se los conecta a una consola telefónica.
- **Servidores de archivos**: nos permiten compartir el material y guardarlo de manera segura, y ofrecen una mayor capacidad de almacenamiento que los equipos de escritorio. Pueden tener conectados varios storage de distintas capacidades.
- **Servidores de seguridad**: se dedican a escanear la red en busca de virus, máquinas desactualizadas por falta de parches del sistema operativo, equipos con determinado software instalado, y muchas otras acciones más.
- **Servidores proxy**: brindan acceso a Internet. En ellos generalmente residen firewalls a los que se les configuran reglas para permitir la navegación por ciertas páginas y bloquear otras. Pueden redireccionar la navegación y mostrarnos algún cartel de advertencia o violación de la política empresarial.
- **Servidores de servidores virtuales**: un solo servidor físico puede contener varios servidores virtuales, pero el usuario final no distinguirá las diferencias. Sólo desde su administración podremos explotar todas sus características. Para obtener más información sobre servidores virtuales, ver el **Capítulo 4** de este libro.
- **Servidores particulares**: se instalan para cada aplicación que utilicemos en la red. Por ejemplo, servidores de workflows, de CRM, de RR.HH., de contaduría, etc.

Los servidores, por sus diferencias físicas, de tamaño y de diseño, también se dividen en **rackeables**, tipo **tower** y **blades**. Los rackeables son aquellos que podemos colocar dentro de un armario con correderas (rack); suelen ser delgados como una laptop de grandes dimensiones. Los servidores tower son los más típicos, parecidos a una PC físicamente, pero más potentes. Por último, los blades son equipos grandes que permiten cambiar o agregar hardware de forma caliente, esto es, mientras el servidor está activo.

Servicios necesarios en una empresa

Al margen de las distintas categorías de servidores que puede tener una empresa, debemos considerar que hay ciertos servicios esenciales que ellos brindan y que son críticos en nuestro trabajo diario. Por ejemplo, un servicio indispensable es el correo electrónico, que debe ser bien administrado y tratado con sumo cuidado. Sin dudas, también es infaltable el servidor de archivos, conocido como **file server**, cuya función es almacenar gran cantidad de información para que los empleados puedan acceder a ella desde cualquier lugar de la red. Brindan un servicio de resguardo, y deben asegurar la integridad y solidez de los datos. En estos servidores podemos administrar los permisos a las carpetas y las **quotas** para cada una de ellas.

Según el tamaño de la empresa, existen otros servicios indispensables. Si es de mediana a grande, debemos pensar en un servidor de backup con su correspondiente red de backup para no saturar el tráfico de la red actual. También debemos tener en cuenta los servicios de un departamento de **bases de datos (DBAs)**, de **helpdesk**, de **seguridad** y de **procesos**.

Otros elementos en la red

Otros elementos que podemos encontrar en una red son las cámaras IP, un estándar en la seguridad de una empresa, que resultan fáciles de instalar y administrar. También, para dar un servicio de búsqueda en las organizaciones, podemos usar equipos como los que ofrece **Google**, que hacen un índice de los archivos de la red.



***Figura 16.** Uno de los equipos que vende la empresa Google. Ésta es la versión full, llamada Google Search Appliance. Existe otra reducida denominada Google Mini.*

Otro elemento en gran expansión son los equipos de telefonía móvil o smartphones, que actualmente pueden tener acceso a la red, a carpetas, a servicios de e-mail y de mensajería instantánea (IM), y que hasta pueden ser dados de alta en el dominio de la empresa. También podemos encontrarnos con dispositivos de **Cloud Computing** (**computación en la nube**). La administración puede volverse engorrosa si no sabemos sobre su existencia, ya que parece otro elemento en la red pero forma parte de una configuración más grande. Este concepto nos permite dejar de lado la pregunta de **dónde se procesa tal sitio web** o **en dónde está almacenada cierta base de datos**. Es importante ver el cloud como un único servicio; atrás pueden encontrarse millones de servidores que se ocupan de procesar los pedidos.

También podemos toparnos con dispositivos que posean la tecnología denominada **grid**, que parecen elementos comunes en la red, pero forman parte de otra configuración mayor. Grid se basa en compartir los recursos de distintos dispositivos que no tienen que ser necesariamente iguales, sino que pueden ser servidores, computadoras de escritorio, PDAs o teléfonos, entre otros. Debemos saber que no importa en dónde se encuentre ubicado el dispositivo: si forma parte del grid, estará compartiendo sus capacidades de cálculo y almacenamiento.

RESPONSABILIDADES PARA ASUMIR

En todos los trabajos existen responsabilidades; en éste, básicamente, es la continuidad del negocio. Esto quiere decir que la empresa debe seguir manteniendo sus servicios y servidores funcionando continuamente. Es preciso tratar de obtener un servicio de 24 horas durante los 365 días del año.

Riesgos en la administración

La administración de servidores es todo un desafío diario, porque nadie sabe resolver todos los problemas que pueden llegar a presentarse. Principalmente, hay que tener sentido común, ser serenos y conscientes. Tratar de automatizar al máximo las tareas frecuentes es una buena idea para estar preparados ante problemas más serios y ofrecer una rápida respuesta. Éste es un trabajo difícil, en el que, en ciertas situaciones, las ventas de la empresa, la conformidad de algún cliente y/o la facturación del mes quedan supeditadas al buen funcionamiento del sistema administrado. El negocio debe continuar para seguir facturando, y depende de nosotros que esto suceda.

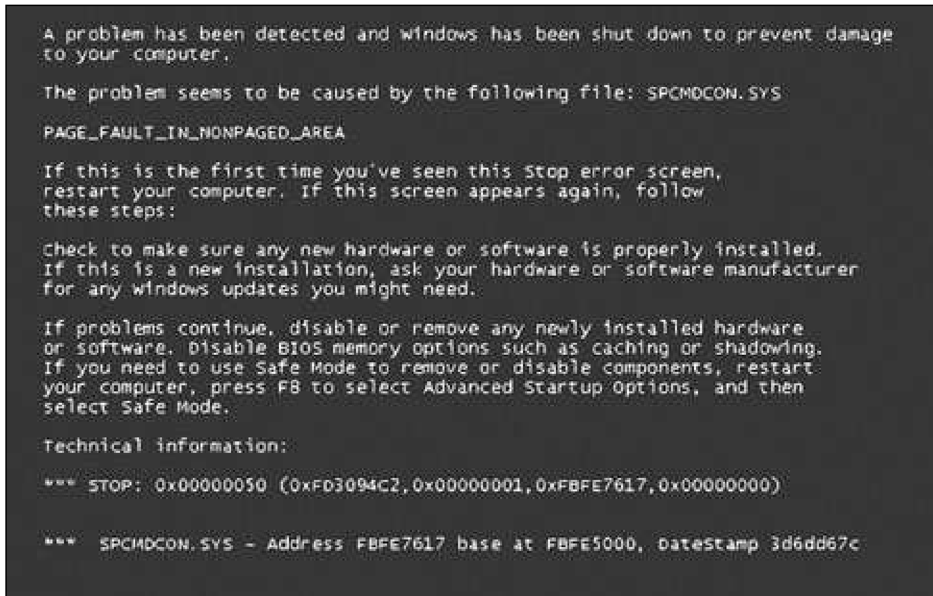


Figura 17. *Ésta es una de las pantallas de error con las que tendremos que lidiar si asumimos la responsabilidad de mantener la continuidad del negocio. Ese error tiene que desaparecer sea como sea.*

Antes de poner un sistema en producción, debemos crear un escenario parecido al real para probar el que vamos a instalar. Esto se denomina **laboratorio**. Por ejemplo,

si queremos instalar una función nueva para el correo en nuestra red, sabemos que necesitamos configurar un servidor Exchange y uno de Active Directory. Entonces, en el laboratorio tendremos que instalar dos servidores que ejerzan esas funciones y una PC para hacer las pruebas del lado del cliente, es decir, del usuario final. Si tratamos cada nueva instalación de esta manera, tendremos la mínima pérdida posible de la continuidad del negocio a la hora de implementar un ambiente productivo. Debemos dedicar horas a estas situaciones de **testeo** previo, para asegurarnos de que todo salga bien. Por ejemplo, si programamos los reinicios de todas las estaciones de trabajo (**workstations**) de la empresa y no tenemos en cuenta que hay personal trabajando fuera de horario, la continuidad del negocio caerá abruptamente.

Ambientes de trabajo

Para cumplir con las exigencias y minimizar los riesgos, debemos mantener un buen ambiente de trabajo, y hay normas internacionales que lo regulan. Dentro de las Normas ISO 9001:2000, por ejemplo, se menciona el ambiente de trabajo como un requisito: **la Organización debe determinar y gestionar el ambiente de trabajo necesario para lograr la conformidad con los requisitos del producto**.

La Norma ISO 9004:2000 se refiere un poco más a qué es el ambiente de trabajo. Cubre aspectos como las metodologías de trabajo, las reglas de seguridad, la interacción social, las instalaciones y la higiene. Los departamentos de recursos humanos deben asegurarse de asignar personas idóneas para realizar estas tareas, de modo de alcanzar un buen estado psicológico del empleado y generar un compromiso constante. También las **normas de seguridad** juegan un papel muy importante en el ambiente del trabajo. Existen normas que prohíben la navegación por las redes sociales o bloquean las comunicaciones IM. Podemos encontrar otra postura de administración, en la cual los directivos piensan y admiten que el empleado pasa más tiempo en la empresa que en su casa, por lo que debería sentirse como en ella. Debemos tener en cuenta que quienes están en esta situación tienen otros privilegios, se mantienen relajados y rinden al máximo.

Relaciones interdepartamentales

Las relaciones con otros departamentos son muy importantes, ya que seremos reconocidos como grupo tanto en las fallas como en los buenos trabajos. Las tareas en equipo son fundamentales, y nos permiten adquirir nuevos conocimientos que, por especializarnos en un tema, no tenemos. La definición de Sistemas dice que **un Sistema es el resultado de la suma de sus partes**. Tenemos que ser una de las partes de él, saber explicarnos, abstraernos de los tecnicismos y dar a entender nuestros pensamientos con palabras sencillas. Preparar una presentación es un buen punto de partida, ya que, junto con un buen discurso, nos permitirán lograr una

clara expresión del problema o situación. La comunicación del grupo sirve para no perder de vista el objetivo de la empresa; el hecho de saber a dónde vamos y cuáles son los proyectos es muy importante para generar un impulso y alcanzar el objetivo planteado. Por eso es clave generar documentación con los pasos que se deben seguir, los responsables, el desarrollo y la historia de ciertos problemas. Por ejemplo, si no se conocieran los teléfonos de los responsables de ciertos sistemas, éstos podrían dejar de funcionar correctamente debido a la falta de atención. Es por eso que las relaciones interdepartamentales son muy importantes y también son parte de nuestro objetivo principal: la **continuidad del negocio**.



***Figura 18.** En el sitio web **www.iso.org/iso/catalogue_detail?csnumber=28692** encontraremos información acerca de la norma ISO 9004:20000.*

… RESUMEN

En este capítulo vimos temas básicos, como qué es una red, qué es un servidor, cuáles son los servicios de una empresa modelo, los riesgos en la administración y las relaciones interdepartamentales. Pudimos entender la importancia de estos factores a la hora de administrar una red, ya que toda la responsabilidad recae sobre nosotros cuando hablamos de la continuidad del negocio. En los próximos capítulos explicaremos cómo se configuran los servidores, nos referiremos a la seguridad, veremos qué es VmWare y sus soluciones de virtualización. También veremos qué es System Center Configuration Manager y cómo estas herramientas pueden ayudarnos un poco más a cumplir nuestro objetivo.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 ¿Cuáles son los cuatro sectores físicos más importantes en un servidor?

2 ¿En cuántas formas pueden categorizarse los servidores?

3 ¿Qué es un blade?

4 ¿Qué es un storage?

5 Enumere los servicios necesarios en una empresa pequeña.

6 ¿Cuál es el significado de la sigla ISO?

7 ¿Cuántas formas de armar un cable UTP existen?

8 ¿Qué significa que el cable esté cruzado?

9 ¿Cuáles son los tres tipos de servidores que hay, hablando físicamente?

10 ¿Qué es cloud computing?

EJERCICIOS PRÁCTICOS

1 Busque en Internet fotografías de servidores y aprenda a distinguirlos.

2 Averigüe las capacidades de un servidor blade.

3 Realice una encuesta sobre los conocimientos de su sector para otros departamentos; esto brindará una noción de cómo los ven desde afuera.

4 Prepare un newsletter para comunicar a los otros departamentos sus novedades semanales.

5 Arme un cable cruzado y uno derecho. Conecte dos computadoras a un switch y compruebe que funcionan de igual manera. Luego conecte dos equipos con los cables y realice comparaciones.

Configuraciones del servidor

Luego de haber visto en el capítulo anterior las necesidades de una empresa y entender qué son los servidores, en éste analizaremos cómo instalar un servidor y sus herramientas, qué es un directorio de dominio y de qué manera generar uno en nuestra red, además de conceptos básicos de seguridad que debemos tener muy en cuenta para la continuidad del negocio. También conoceremos algunas aplicaciones de ejemplo que nos ayudarán a dar estos servicios.

¿CÓMO INSTALAR UN SERVIDOR?

Desarrollaremos a continuación los conocimientos que debemos tener para realizar la instalación de un nuevo equipo en nuestra empresa. Este proceso comienza al sacar el servidor de su caja, y concluye cuando se tiene un sistema operativo funcionando con normas de seguridad aplicadas y con el programa correspondiente para brindar el servicio en la red. Entonces, detallaremos primero la instalación física de un servidor, y luego pasaremos a la instalación lógica.

Instalación física

El primer paso es encargar el servidor al proveedor. Para hacerlo, es necesario elegir bien el equipo, según las prestaciones requeridas y los precios del mercado. Luego, el proveedor nos entregará el servidor correspondiente con las características pedidas, junto con los discos de instalación, las herramientas de aplicaciones y los drivers, todo dentro de una caja sellada. Los racks, donde instalaremos los equipos (como vimos en el **Capítulo 1**), son armarios metálicos en los que irán colocados los servidores, routers, switches y pacheras. Veremos a continuación cómo instalar un servidor en un rack.

■ Instalar un servidor en un rack — PASO A PASO

1 Desembale la caja que recibió del proveedor. Saque todos los elementos, y aparte las guías, los tornillos, los CDs de instalación y el servidor.





►

2 Elija un lugar apropiado en el rack en donde entre físicamente el servidor, y haya energía y ventilación suficientes. Coloque las guías en las paredes del rack.

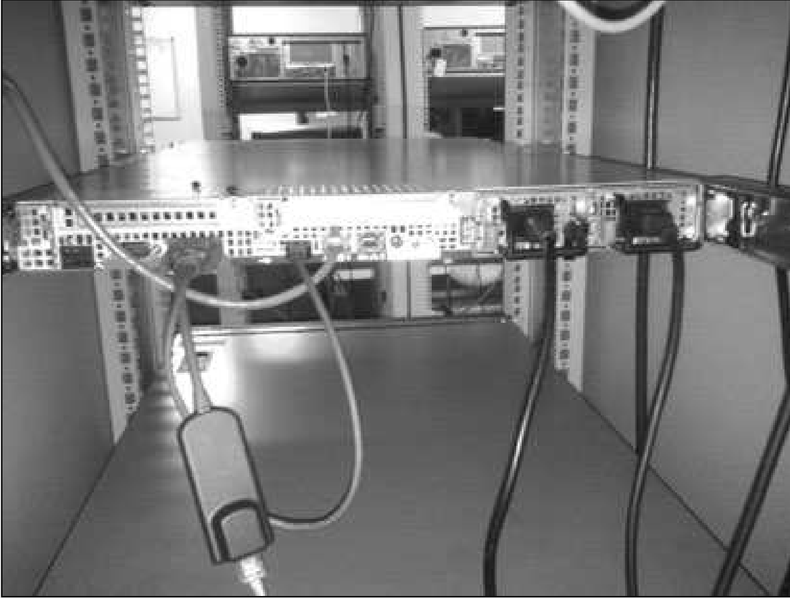


3 Tome el servidor, fije las partes de las guías correspondientes a sus costados y colóquelo sobre las guías en el rack. Corra las trabas y empújelo hacia atrás.



►

► 4 Enchufe los cables de alimentación, uno por fuente, y conecte los cables de red. También coloque los cables de la consola para el monitor, teclado y mouse. Luego enciéndalo y verifique la consola.



Acabamos de ver cómo instalar un equipo en un rack, pero si no tenemos un rack, deberemos comprar uno, porque no es muy apropiado colocar el servidor en cualquier lugar del centro de cómputos. Un dato interesante es que existen normas que los fabricantes deben cumplir y que nosotros deberemos tener en cuenta. Éstas nos aseguran que tendremos medidas estándar para colocar cualquier equipo en cualquier rack. Si esto no fuera así, nos veríamos en problemas. Tener conocimiento sobre esto nos ayudará a elegir mejor nuestros racks para instalar los servidores de la mejor manera posible. Debemos tener cuidado no sólo en la elección del rack, sino también en contar con la energía suficiente. Esto significa que hay que buscar

III DMZ (ZONA DESMILITARIZADA)

Se trata de una red intermedia, ubicada entre la red interna de la empresa y una externa, por ejemplo, Internet. Los equipos en la red interna se comunican hacia los equipos de la DMZ y hacia la red externa, pero no se permite la comunicación desde la red externa hacia la interna. Los equipos en la DMZ dan servicio a la red externa y, al mismo tiempo, protegen la interna.

un lugar en donde haya energía disponible para conectar el equipo, donde haya puestos de red libres y donde haya un lugar que cumpla con las normas de seguridad necesarias. Si el servidor es de desarrollo, tal vez tengamos una sala sin demasiada seguridad en donde colocarlo; mientras que si es productivo o crítico, probablemente dispongamos de otro sitio, otro centro de cómputos o una sala más segura de lo normal. Llamamos servidor de desarrollo a aquel equipo que se utiliza para testear aplicaciones o desarrollarlas. En cambio, un servidor productivo es el que tiene aplicaciones que brindan servicios a todos los usuarios de la red. Es necesario tener resguardo de todos los servidores, pero, principalmente, de los productivos. Cualquier auditoría seria nos pedirá tener un plan de recuperación de desastres, o DRP (*Disaster Recovery Plan*) por cada servidor productivo.

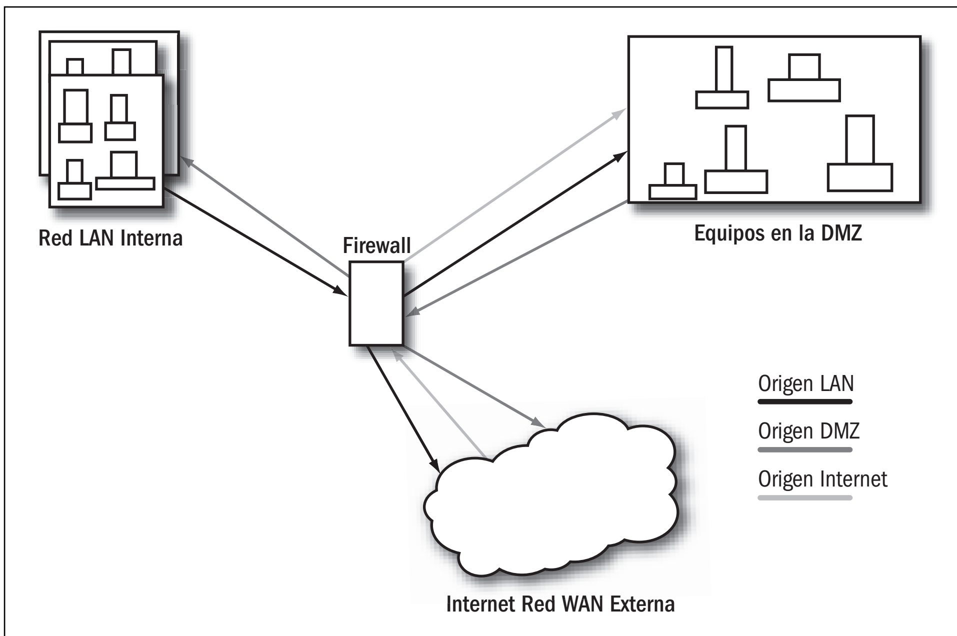


Figura 1. *La DMZ se utiliza para dar acceso a ciertos sistemas de consulta externa, sitios web de la empresa, etc. Es uno de los tres sitios en donde puede estar la información empresarial, además de la red interna e Internet.*

Los centros de cómputos cuentan con grandes sistemas de refrigeración que brindan una temperatura constante de unos 22° grados Celsius, generalmente. La ubicación del servidor en el rack tiene que ser aireada, y debemos documentarla y numerarla para lograr la rápida localización del equipo.

Una vez que hayamos instalado el servidor en el rack, será necesario que pasemos a la configuración de la red, para lo cual tenemos que habilitar un puerto en el switch y colocarlo en la subred que corresponda. Luego, conectamos los cables al equipo y nos fijamos si la luz de la placa de red enciende.

Instalación lógica

Cuando hablamos de instalación lógica, nos referimos a la instalación de las herramientas del servidor, del sistema operativo y de las aplicaciones y/o servicios que corresponda. Las herramientas del servidor hoy en día vienen preinstaladas. Una muy importante es la de configuración del **array**, o el conjunto de discos del cual disponemos. Ellos pueden estar en el servidor o conectados a él en una unidad de storage. El array se organiza en niveles de **RAID** (del inglés *Redundant Array of Independent Disks*, o conjunto redundante de discos independientes). Las ventajas que esto representa, en vez de tener toda la información en un solo disco, son mayor integridad, rendimiento, tolerancia a fallos y capacidad. Debemos tener en cuenta cuál será el fin del servidor, las necesidades y la criticidad. Existen distintos niveles de RAID, que varían según su configuración y el grado de resguardo que se da a los datos. Los más usados son 0, 1 y 5. Veamos cuáles son sus principales características.

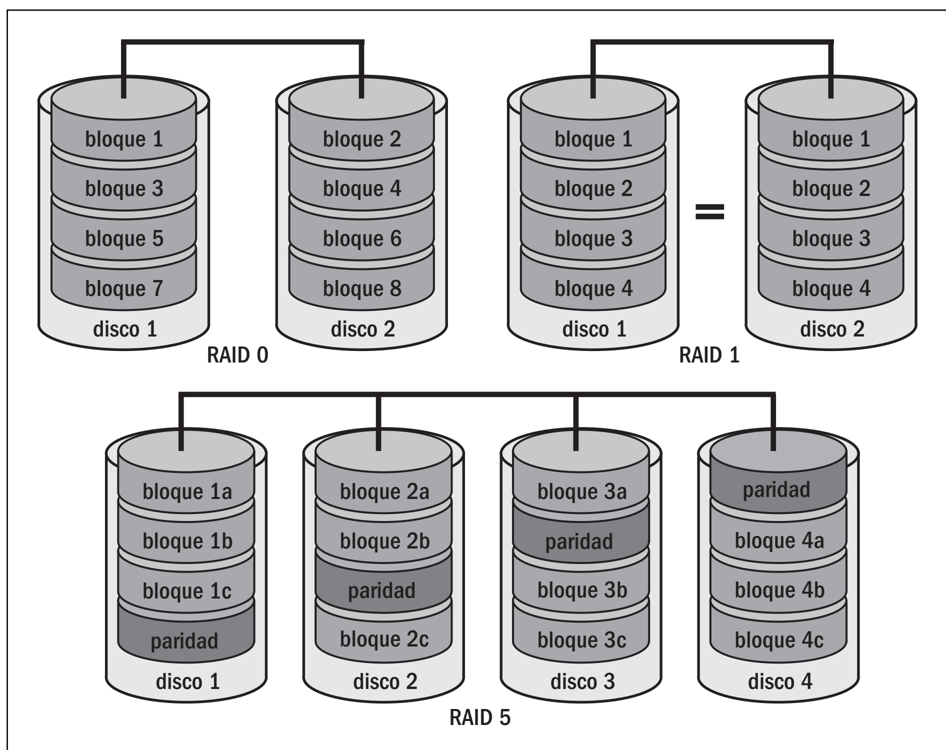


Figura 2. *En el gráfico podemos ver las diferencias entre los tipos de RAID. El RAID 0 es uno solo dividido, el RAID 1 es un espejo, y el RAID 5 es dividido pero con un control extra para que no se corrompan los datos.*

- **RAID 0**: se utiliza para aplicaciones de desarrollo, no críticas. Este tipo de RAID utiliza el grupo de discos que tengamos como un solo disco. Si alguno se rompe, perderemos la información, y el RAID se romperá sin posibilidad de recuperarlo.

Nos permite tener mayor capacidad que un solo disco grande, pero no ofrece redundancia. Nos da mayor rendimiento y podemos reutilizar discos de distintas capacidades para crearlo. Los sectores del disco donde se guarda la información están distribuidos en el grupo de discos. La lectura de los datos se hace de forma simultánea. Por ejemplo, un archivo de texto puede ocupar varios sectores de disco; al almacenarlo en un RAID 0, puede ser que dichos sectores grabados estén en un solo disco o en más de uno. En este último caso, la velocidad de lectura aumenta con respecto a un solo disco grande. La velocidad de transmisión de datos será mejor que con un solo disco.

- **RAID 1**: funciona como un espejo entre los discos. Los grupos de discos se conforman con números pares, y el número mínimo de discos es dos. En este caso, todo lo que sea escrito, modificado o borrado en uno será igualmente escrito, modificado o borrado en el otro. Al igual que el RAID 0, el tiempo de lectura disminuye; es decir, la velocidad a la que podemos leer los datos desde los discos es mayor que si contáramos con un solo disco (tardaremos menos en leer un dato). Podemos tener un resguardo de otro disco almacenando una copia de seguridad. Esto se realiza marcando uno de los discos como inactivo, sacándolo del servidor o storage, y colocando otro disco nuevo. El sistema de RAID se ocupará de reconstruirlo y podremos guardar el disco que saquemos en un armario. No es la mejor solución de backup, pero es mejor que no tener ningún resguardo y se realiza muy fácilmente.
- **RAID 5**: es el más utilizado porque brinda redundancia y velocidad. Permite utilizar el 80% de la capacidad del conjunto de discos. Se necesitan aunque sea tres discos para formarlo, y en caso de que uno falle, el servidor seguirá funcionando hasta que lo cambiemos. Los sectores se graban de manera distribuida, mezclándose con sectores de paridad utilizados para el control. Si un disco falla, se copian sus datos a los otros discos sin que el servidor deje de funcionar.

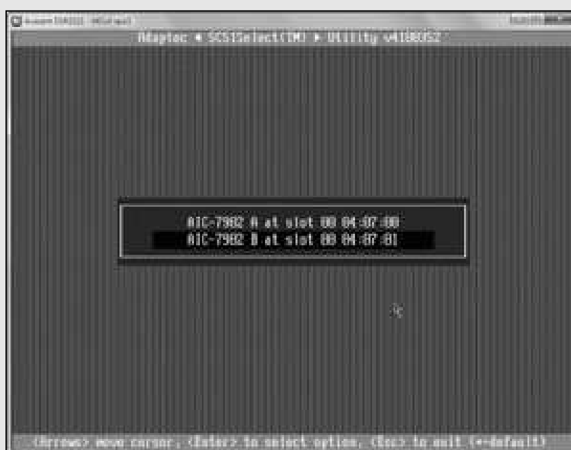
TIPO DE RAID	DETALLES
RAID 0	Se graban los datos distribuidos, pero sin tolerancia a fallos.
RAID 1	Se graban los datos en espejo; si un disco falla, el otro sigue funcionando.
RAID 2	Utiliza un algoritmo complicado que demanda muchos cálculos a la CPU. Es lento y se requieren discos especiales. Permite acceso en paralelo.
RAID 3	Usa un disco de control de paridad, de esta forma permite el acceso en paralelo, pero todos los discos deben funcionar al unísono.
RAID 4	Es parecido al RAID 3, pero es posible acceder a los sectores de forma individual. No es necesario leer de todos los discos al mismo tiempo.
RAID 5	Se graba en forma distribuida con datos de paridad para controlar los datos; si cualquier disco se rompe, el sistema sigue funcionando.
RAID 6	Funciona de manera parecida al RAID 5, pero permite que se rompan dos discos. Debemos tener en cuenta que es muy poco utilizado debido a su elevado costo.

***Tabla 1.** Niveles de RAID junto con sus respectivos detalles.*

Las herramientas de configuración del RAID vienen preinstaladas o en los CDs de instalación que están en la caja del servidor. Una muy utilizada es la de la empresa **Adaptec**, presente, por lo general, en equipos SUN o HP. A continuación, veremos cómo configurar un RAID 1 del tipo espejado, para tener una mínima configuración con discos redundantes y a prueba de fallos.

■ Configurar un RAID 1 (espejado) con Adaptec PASO A PASO

1 Tome los discos para el array y colóquelos en el equipo. Encienda el equipo y oprima la combinación de teclas **CTRL + A**. Elija una de las placas controladoras SCSI de los discos que tiene su equipo para trabajar. Si no reconoce los discos, elija la otra.

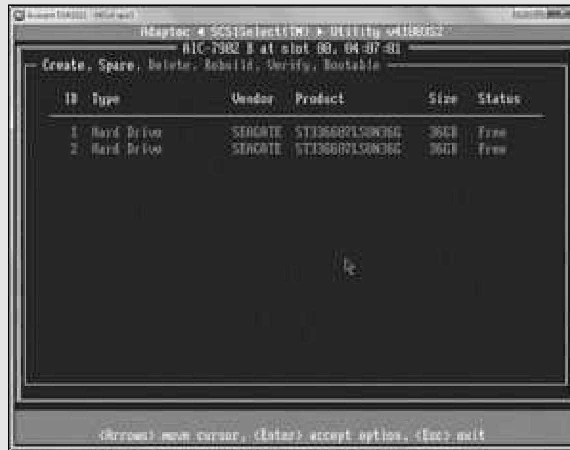


2 Escoja la opción **Configure/View HostRaid Settings** para ver o configurar el RAID. Se mostrarán los detalles si hay algún RAID ya realizado.





3 Verá los discos reconocidos. Oprima **ALT + C** para generar el RAID.



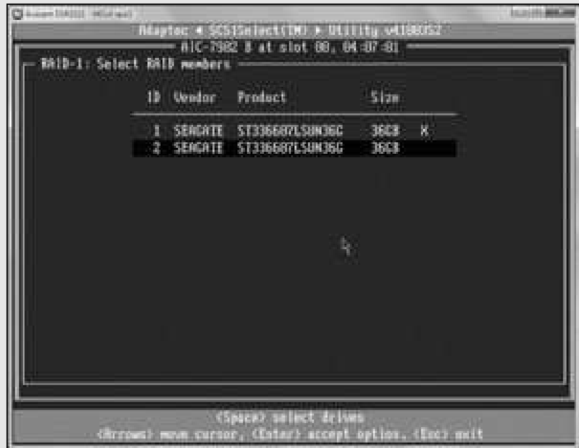
4 Elija el tipo de RAID que va a crear, que dependerá de la cantidad de discos. Para este ejemplo, es **RAID-1 (Fault Tolerance)**.



III VPN

Es un tipo de red, cuya abreviatura proviene del inglés **Virtual Private Network**. Se utiliza para extender una red privada sobre una red pública como es Internet. La implementación de una red de estas características debe proporcionar y garantizar autentificación, integridad y confidencialidad. Esta clase de conexiones es muy utilizada para acceder en forma remota a una empresa.

5 Oprima la **barra espaciadora** para seleccionar los discos que conformarán el RAID. En caso de tener dos discos, marque ambos.



6 Escriba un nombre para el RAID que no sea muy complejo y oprima la tecla **ENTER**.



III IMAGEN ISO

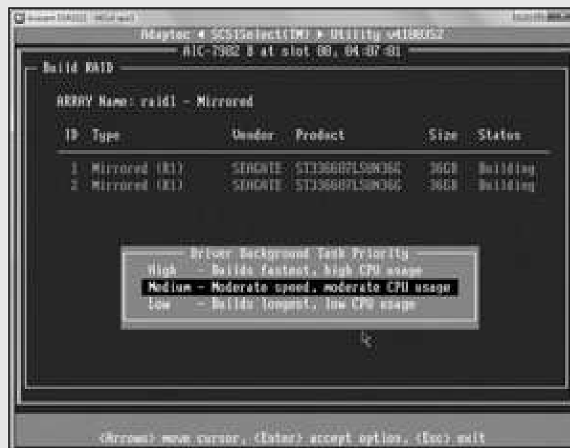
Una imagen ISO es una copia exacta de un disco con sus particiones, unidades y software instalado. Es una réplica de un sistema de archivos. Este tipo de imagen se rige por la norma ISO 9660, que le da el nombre. Fue creada en 1986 y especifica el formato para almacenar los archivos en un disco compacto. Esta norma permite que los archivos sean leídos por distintos sistemas operativos.

►

7 Para continuar será necesario que cofirme la operación las veces que sean necesarias hasta ver el mensaje **Build Completed**.



8 Elija la velocidad y el consumo de CPU para crear el RAID. Cuando termine, verifique el RAID y salga de la aplicación apretando la tecla **ESC**. Reinicie el equipo y comience la instalación del sistema operativo.



Una vez que configuremos el array, debemos pasar a la instalación del **sistema operativo**. Más allá de cuál instalemos, los pasos son básicamente iguales a los que debemos realizar para instalar un sistema en una PC de escritorio: se analizan y construyen las particiones necesarias, se crean las unidades lógicas, se formatean los discos con el sistema de archivos por utilizar, y se comienza la instalación. Tanto en Windows como en Linux, podemos instalar un sistema operativo desde cero

colocando el CD correspondiente, iniciando el equipo con esta unidad y siguiendo los pasos. También hay otro tipo de instalación que se realiza mediante imágenes ISO, copiando algún sistema preinstalado a los nuevos discos.

Seguridad básica

El tema principal en cuestión de seguridad es contar con un **plan de contingencias**. Por lo general, éste es realizado por un representante del área de higiene y seguridad o ingeniero civil para resguardo físico del lugar. El plan nos dice qué hay que hacer en caso de desastres, dónde están las salidas, cómo se accionan los equipos para apagar el fuego y todos los pasos por seguir. Nosotros, como administradores, debemos contar con nuestro propio plan de recuperación de desastres. Físicamente hablando, tenemos que disponer de un grupo electrógeno de soporte, un grupo de equipos UPS y dos fases conectadas al suministro de energía.

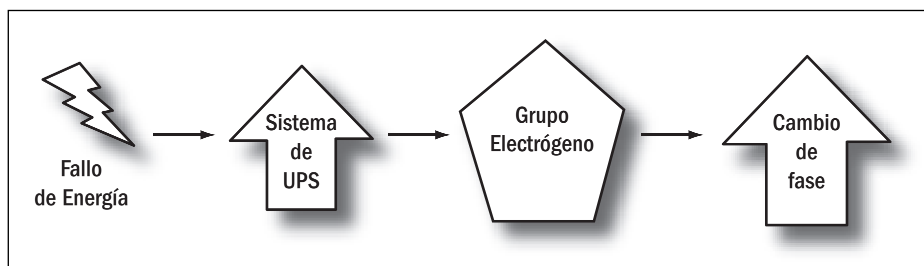


***Figura 3.** Pasos en los que deberíamos pensar cuando se produce un corte de energía: primero nos resguardan los equipos **UPS**; luego, el **grupo electrógeno** y, por último, se realiza un **cambio de fase** en la red de energía.*

Otro aspecto para tener en cuenta es el acceso al centro de cómputos. Es necesario contar con un registro de entradas donde se guarde la identificación de quién ingresó y el horario correspondiente. Para este fin se utilizan tarjetas magnéticas con un software no muy complejo y puertas de seguridad magnéticas. En grandes centros de cómputos de clientes, la seguridad es mucho más estricta. La entrada se otorga mediante mecanismos de reconocimiento biométricos, de voz y escaneo de iris.



UPS (UNINTERRUPTIBLE POWER SUPPLY)

Una UPS es un dispositivo que contiene baterías para brindar energía en forma ininterrumpida. Dependiendo de la cantidad de baterías con que cuente, ofrecerá más tiempo o menos tiempo; en general, son un par de horas. También tienen funciones de estabilización de la energía filtrando aumentos y caídas de tensión.

DIRECTORIO DE DOMINIO

Los directorios de dominio nos permiten administrar los objetos de la red y sus relaciones. En ellos administramos usuarios, servidores o máquinas de escritorio, guardamos sus informaciones personales y de oficina, les otorgamos permisos, los agrupamos y les damos seguridad. El sistema más utilizado en la actualidad es **Active Directory** (directorio activo de ambientes Microsoft). Éste es el sistema que explicaremos a continuación, pero también hay otros Linux o UNIX, como el **NIS**, muy empleado en organizaciones basadas en servidores con esta infraestructura.

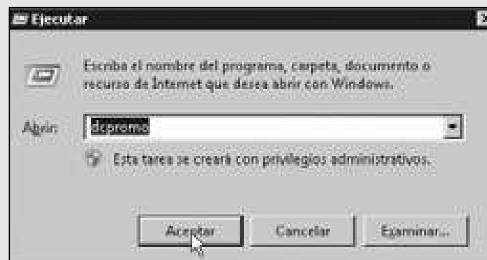
¿Qué es el directorio de dominio?

Llamamos directorio de dominio o, simplemente, dominio a la infraestructura que administra un grupo de objetos que cumplen con determinadas reglas de seguridad y configuraciones dentro de la empresa. Son equipos interconectados que comparten información administrativa centralizada; se los llama controladores de dominio. Puede haber varios dominios o tan sólo uno, separados totalmente o con relaciones de confianza entre ellos. Estas relaciones crean un vínculo de seguridad de cada uno de los dominios que la componen. Debemos saber que el dominio está conformado por objetos, los cuales pueden ser máquinas, usuarios, grupos, reglas de seguridad y varios otros servicios que se detallarán más adelante en este capítulo, en el apartado referido a configuraciones de red.

El directorio guarda toda la información de seguridad de la compañía. Cuenta con una base de datos para almacenarla. Podemos expandir esta base y hacerla crecer, si queremos agregar componentes al dominio, como componentes de Communicator, de SharePoint, de Exchange, etc. Ahora veremos cómo crear un dominio Active Directory con Windows Server 2008.

■ Crear un dominio Active Directory — PASO A PASO

1 En primer lugar, diríjase al menú **Inicio** y haga clic en **Ejecutar**. Luego escriba **dcpromo** y oprima el botón llamado **Aceptar**.



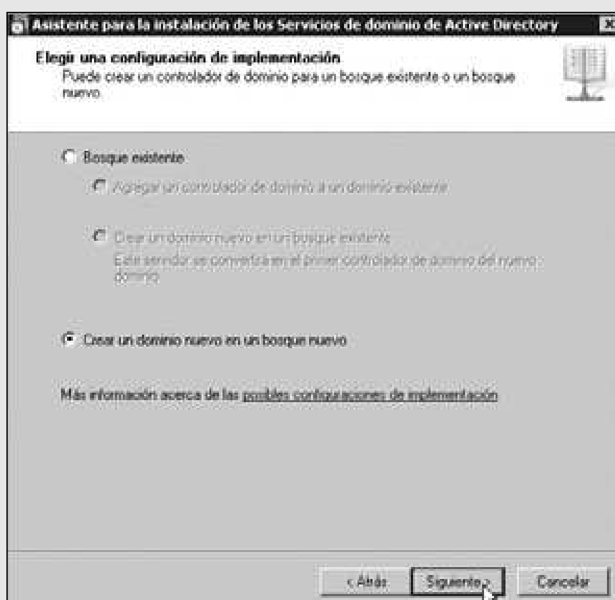
▶

▶

2 Se abrirá un asistente para crear el dominio; presione **Siguiente**. Se mostrará un informe de compatibilidad; oprima **Siguiente**.



3 Elija la opción **Crear un dominio nuevo en un bosque nuevo**. La otra opción se elige en caso de querer extender un dominio ya existente.



▶

▶

4 Este paso es importante: elija un buen nombre de dominio y escríbalo; por lo general, representará a la empresa.



5 Para continuar, establezca el nivel funcional del bosque, si sólo va a tener servidores 2008 o también 2003 Server.



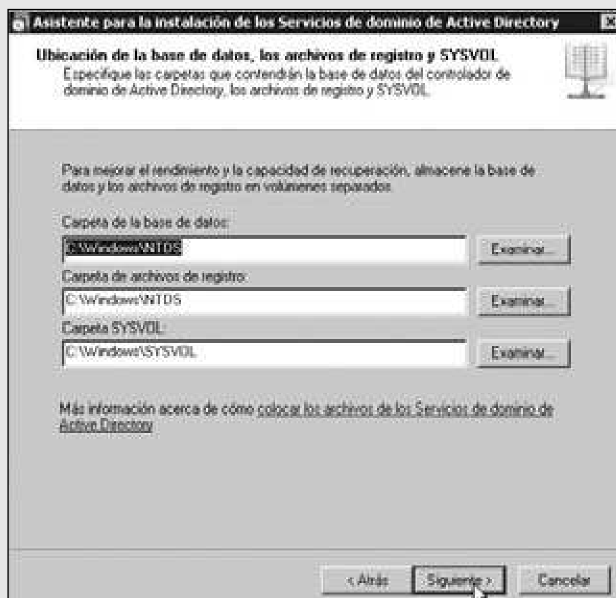
▶

▶

6 Seleccione la opción **Servidor DNS** si así lo desea. Recibirá una advertencia al apretar en **Siguiente**, pero de todos modos haga clic en **Sí**.



7 Seleccione el lugar donde se guardarán los archivos de la base de datos. Podrá cambiar la ubicación solamente con esta opción.



▶

►

8 Establezca una contraseña para recuperar el dominio en caso de desastres. Oprima el botón denominado **Siguiente**.



9 Una vez que terminó de armar el dominio, pulse en el botón llamado **Finalizar**. El sistema le pedirá que reinicie el equipo.



La infraestructura del dominio puede estar compuesta por uno o varios servidores, los cuales replican sus datos y se mantienen actualizados unos con otros. En empresas grandes, hay que distribuirlos según la ubicación de los usuarios, quienes, al entrar en la red, deben utilizar sus nombres de usuarios de red y claves para que el controlador de dominio les brinde sus datos y permisos. Si este servidor está muy alejado de su ubicación, la entrada a la red tal vez sea muy lenta.

Administración del directorio

Ya entendimos qué es un directorio de dominio; ahora aprenderemos a administrarlo. En la consola de administración del directorio para Active Directory se ve un árbol con distintas ramificaciones llamadas **unidades organizacionales** o, simplemente, **OU**. Es importante saber que cada OU es una carpeta que contiene los objetos del dominio. A continuación, veremos cómo crear un nuevo objeto usuario para que un empleado pueda acceder a la red.

■ Crear un nuevo usuario de red en el dominio — PASO A PASO

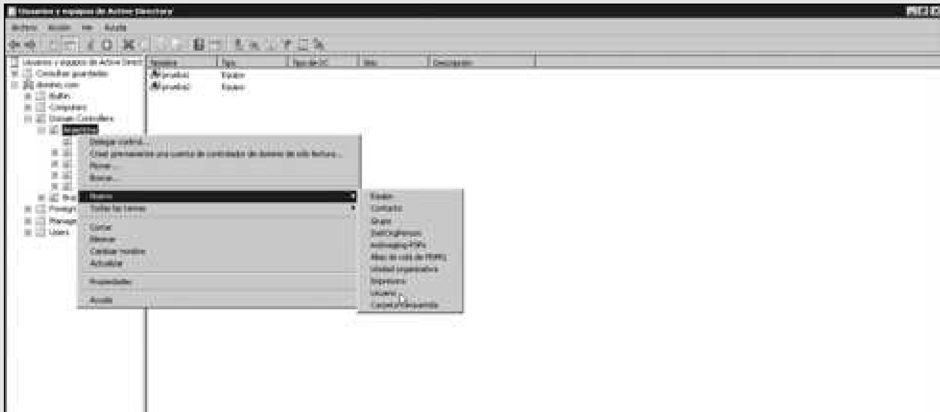
1 Vaya a la consola de Active Directory desde el menú **Inicio/Herramientas administrativas/Usuarios y equipos de Active Directory**.



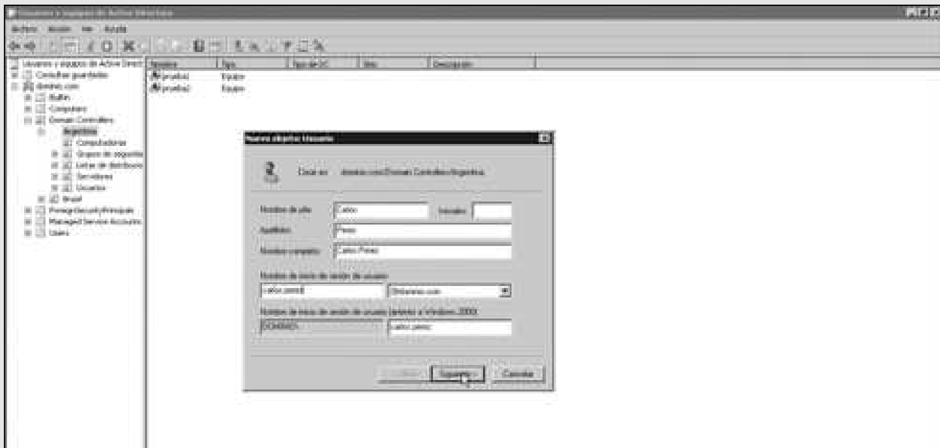
►

▶

2 Para continuar, diríjase a la OU donde quiere que esté el usuario, haga clic derecho del mouse sobre ella y elija **Nuevo/Usuario**.



3 Complete los datos del usuario y oprima el botón **Siguiente**. Ingrese la contraseña, presione **Siguiente** y, luego, pulse **Finalizar**.



III LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)

Es un protocolo utilizado para ingresar en los directorios de dominio. Fue creado en el año 1993 en la Universidad de Michigan. Define el método para acceder a los datos en el servidor, pero no, la manera en que se almacena la información. El usuario puede conectarse, buscar información, comprarla, insertar datos, cambiarlos y/o eliminarlos.

Después de la creación de un nuevo usuario, debemos asignarle permisos y listas de distribución, pero con los datos de usuario y contraseña, el empleado ya puede trabajar. Los objetos usuario tienen, de forma estándar, una solapa de datos personales, otra de ubicación, membresía de grupos y datos de la cuenta de red; con las herramientas de Exchange pueden visualizarse las solapas de correo en donde figurarán las direcciones de e-mail. Los grupos de cada usuario pueden ser de seguridad o de listas de distribución. Los primeros se utilizan para agrupar distintos usuarios y otorgarles seguridad en conjunto. Por su parte, los segundos, para tener una dirección de correo en común para varios usuarios.
Si queremos un poco más de detalles de los objetos que los brindados por la consola de Active Directory, podemos consultar la herramienta llamada **ADSI Edit**, también de Microsoft, incluida con las herramientas administrativas del sistema operativo. Con ella, tendremos a nuestro alcance todos los atributos avanzados de los objetos. Es muy importante entender esta herramienta, porque puede servirnos para solucionar importantes inconvenientes.

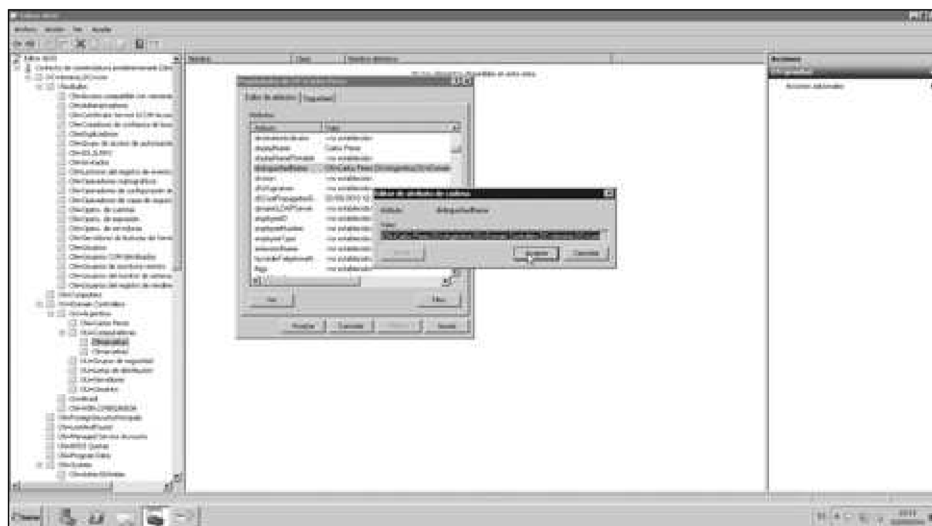


Figura 4. *ADSI Edit es una herramienta de la firma Microsoft para usuarios avanzados, pero existen otras muy buenas también, como LDAP Admin o AD Manager.*

WORKFLOWS

Los workflows son flujos de trabajo, que se componen de tareas, procesos, aprobadores y ejecutadores de las tareas, de principio a fin. Se utilizan en las organizaciones para realizar el control de distintas operaciones, así como también para automatizar algunas de ellas. Son muy importantes para las auditorías, ya que brindan un historial de las acciones que se realizan en una empresa.

CONFIGURACIONES DE RED

Es fundamental tener un conocimiento amplio sobre las configuraciones de red cuando pretendemos realizar la administración de servidores y aplicaciones en entornos corporativos. Esto es importante ya que todos los elementos de la red se comunican gracias a ciertos protocolos, dispositivos y configuraciones que debemos tener en cuenta. A veces, se hace difícil distinguir la causa de un problema de comunicación, pero si poseemos los conocimientos necesarios, podremos defendernos mejor; en vez de esta forma será posible que encontremos la causa de la dificultad y llegaremos a cumplir de buena manera el objetivo principal, que planteamos desde el principio del libro: lograr la continuidad del negocio.

Conceptos fundamentales

En la administración de servidores, debemos conocer qué es un rango IP, y entender qué función cumple un DHCP, un DNS, un router, un switch, etc. Todo esto es necesario para comprender de qué forma se interconectan nuestros equipos y, también, los usuarios finales, quienes consumirán el servicio brindado.
Los rangos de IP son las direcciones en la red que tendrán los dispositivos que se conecten a ella. Cada equipo contará con una dirección IP, que será su identificación personal, su documento de identidad en la red. Haciendo una analogía con la realidad, si tenemos una ciudad llena de servidores, la dirección IP sería la dirección postal unívoca para cada uno. Así podremos conectar computadoras, servidores, impresoras, teléfonos, cámaras, un switch, un router, etc.
Las direcciones IP se componen de cuatro números separados por un punto, que van del 0 al 255. Hay varias clases de direcciones IP, que se dividen por rangos y por redes. Para distinguir las redes, utilizamos máscaras de red, que se configuran en el mismo momento en que se da una dirección IP al equipo. La máscara de red nos dice a qué red pertenece esa máquina. También se divide con cuatro números (al igual que la dirección IP), pero se coloca el 255 en el que representa la red, y el 0 en donde se representen los números posibles de los hosts. Por ejemplo, si tenemos una dirección 10.3.5.27 con una máscara 255.0.0.0, sabremos que pertenece a la red 10.0.0.0 y se refiere al host 3.5.27.

CLASE	RANGO	CANTIDAD DE REDES	CANTIDAD DE HOSTS	MÁSCARA
A	1.0.0.0 - 127.255.255.255	126	16777214	255.0.0.0
B	128.0.0.0 - 191.255.255.255	16382	65534	255.255.0.0
C	192.0.0.0 - 223.255.255.255	2097150	254	255.255.255.0
D	224.0.0.0 - 239.255.255.255			
E	240.0.0.0 - 255.255.255.255			

***Tabla 2.** Clases de direcciones IP.*

Dentro de todas las posibilidades de numeración de las direcciones IP, hay algunas especiales que se utilizan de forma estándar para identificar ciertas configuraciones. Estas redes especiales, rangos y usos reservados están definidos por la agencia **ICANN**. Algunas restricciones establecidas sobre ciertas direcciones pueden ser, por ejemplo, la dirección 0.0.0.0, que se utiliza para equipos que todavía no tengan una dirección asignada; es el caso, por ejemplo, de un equipo que se encuentra arrancando. La dirección 127.0.0.1 se emplea para pruebas locales de la placa de red, llamadas **pruebas de retroalimentación**. También dentro de cada clase de red hay direcciones privadas que no deben usarse. Entonces, por ejemplo, una PC que tenga la dirección 192.168.0.4, sabremos que pertenece a la red 192.168.0.0.
También, dentro de una red podemos crear subredes, utilizando el número de hosts para ese fin. Así, teniendo la IP 172.17.1.3 con máscara 255.255.0.0, sabremos que la red es la 172.17 y podremos dividir el tercer número en 255 redes. Entonces, el equipo pertenecería a la subred 1, y el host sería el número 3. Nuestra red estará dividida, por lo tanto, en distintas subredes, las cuales podremos distinguir y administrar por separado. Podremos crear nuestras subredes para identificar departamentos, por pisos, por ciudades o como se nos ocurra.
De cada lado de una red hay un router; recordemos que es el dispositivo utilizado como puente entre las redes. Las direcciones IP pueden ser estáticas o dinámicas. Las primeras no cambiarán a lo largo del tiempo, y será nuestra tarea administrarlas en una planilla o una base de datos. Las segundas pueden ir variando a lo largo de los días y se utilizan, generalmente, para equipos de escritorio. El encargado de administrarlas es el servicio de DHCP. También podemos intervenir nosotros reservando cierta dirección, siempre para un dispositivo determinado.
El DNS es el encargado de convertir las direcciones IP en nombres, y éstos, en direcciones IP. Cuando accedemos a una máquina llamada **usuario1**, es el DNS quien resuelve el nombre en una dirección IP. También es muy utilizado para los sitios web: el nombre del sitio al cual nos dirigimos es convertido en una dirección IP por el DNS, para que éste sepa a qué servidor nos referimos y redirigirnos a él.
Los dispositivos se manejan por direcciones IP, y no, por nombres. El nombre es una abstracción de la realidad para lograr un mejor entendimiento por parte del ser humano. Para comprender esto un poco mejor, siempre que escribamos una dirección de

III ICANN

Esta agencia es una organización sin fines de lucro creada en el año 1998 para realizar la tarea internacional de regular el uso de las direcciones del protocolo IP. Normaliza el uso de direcciones privadas y públicas, administra los rangos y las clases en forma internacional, y se dedica a preservar la estabilidad de Internet por medio de procesos basados en el consenso.

web –por ejemplo, **www.google.com**–, es un DNS en nuestro proveedor de Internet el que lo transforma en una dirección IP del tipo 200.90.198.4, para poder conectarse al servidor de Google y mostrarnos la pantalla del famoso buscador.

Configuraciones básicas

Ya conocimos los términos que nos ayudarán a administrar nuestro entorno; veamos ahora qué herramientas tenemos para realizar las configuraciones. En un principio, contamos con las distintas consolas de DNS y DHCP, principalmente, que manejaremos con una consola MMC (*Microsoft Management Console*). Ésta es una consola que agrupa a muchas otras, que se pueden combinar y agregar según nuestras necesidades. La consola de DNS nos permite administrar los distintos nombres y direcciones IP en una red. Definimos **zonas de búsqueda directa** y **zonas de búsqueda inversa**. En esta consola debemos definir los dominios de los sitios web, administrar y pensar la mejor manera de organizarlos. Por ejemplo, podemos tener un sitio principal que se denomine **intranet.com** y, luego, subdominios de este último para organizar la navegación de una forma correcta y concisa. Un subdominio podría ser **usuarios.intranet.com**.
En el próximo Paso a paso veremos la forma adecuada de realizar la configuración de un registro de DNS con una IP y un nombre específico.

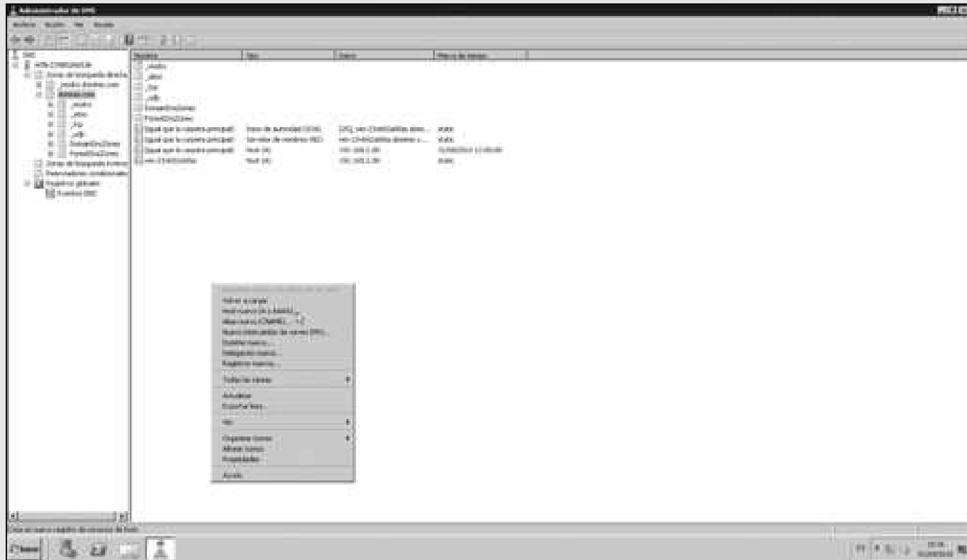
Configurar un registro de DNS — PASO A PASO

1 Diríjase a las **Herramientas administrativas** y abra la consola de **DNS**.

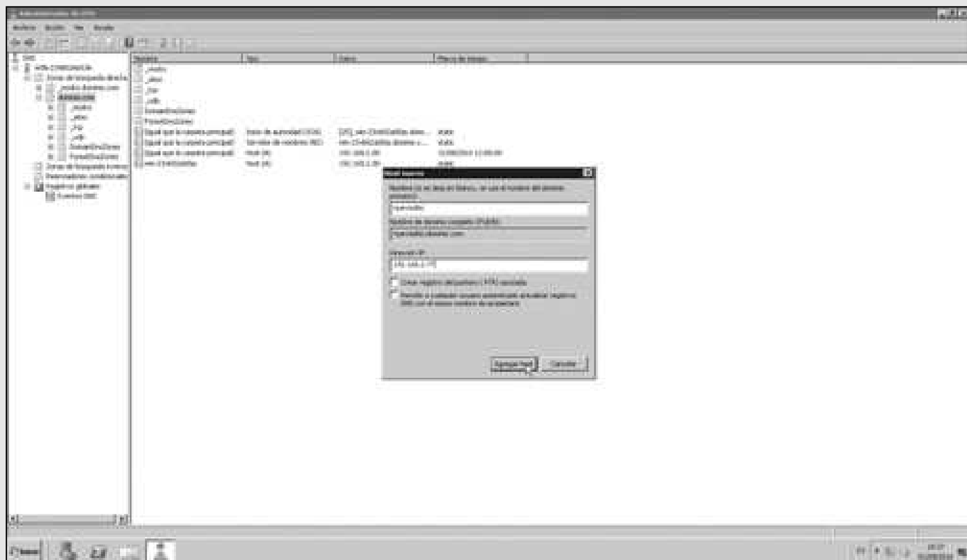


▶

2 Vaya al lugar donde quiere crear el registro; si es parte de su dominio, diríjase a **dominio.com** y, en el lado derecho de la pantalla, haga clic derecho del mouse y elija **Host nuevo(A o AAAA)**.



3 Para continuar, deberá escribir el nombre del registro de DNS y la IP que corresponda. Luego haga clic sobre el botón denominado **Agregar host**, que se encuentra en la ventana abierta; de esta forma finalizará la tarea.



La consola de DHCP es el lugar en donde configuraremos las direcciones IP automáticamente y también donde podremos realizar reservas para determinados equipos. En esta ubicación será posible definir las distintas subredes y también los rangos para todos los dispositivos que deseemos.

Figura 5. *Vemos una consola de DHCP, donde se distinguen las IP brindadas automáticamente y las reservas que hayamos realizado.*

En la consola de DHCP podremos ver las direcciones brindadas: por ejemplo, los equipos conectados a la red en forma automática con sus nombres y respectivas direcciones MAC. Debemos tener en cuenta que las direcciones denominadas MAC son los números que identifican en forma unívoca a un dispositivo de red determinado. Es un número provisto por el fabricante de hardware, que no se puede repetir en el mercado. Si queremos realizar una reserva de una dirección IP para cierta máquina, debemos tomar, por ejemplo, la IP dada en forma automática y crear un registro en la carpeta de reservas con la MAC correspondiente. Esto hará que, cuando el equipo se conecte otra vez a la red, el DHCP le brinde siempre la misma dirección IP. Este sistema es muy utilizado en equipos que deben tener puertos abiertos en firewalls o permisos estrictos para sus redes.

APLICACIONES EN UNA RED CORPORATIVA

Ya vimos la manera de instalar un servidor, cómo encontrarlo en la red y cómo administrarlo con un dominio activo. Ahora, retomando lo explicado en el **Capítulo 1** sobre el tema de los servicios necesarios para una empresa, describiremos algunas aplicaciones que nos permitirán dar esos servicios en nuestra red. Veremos algunas aplicaciones para la administración y la seguridad como introducción al **Capítulo 3**, donde analizaremos en forma más detallada ciertas políticas de seguridad, antivirus y firewalls.

Importancia del correo en la empresa

El correo electrónico es muy importante, como ya mencionamos anteriormente. En él se maneja casi toda la información de la empresa y nos permite estar conectados. Hay muchos motores de correo que se utilizan, pero el más conocido es **Microsoft Exchange** debido a su integridad con el Active Directory, a su solidez, trayectoria y confianza en el mercado. Algunas empresas optan por mantener su correspondencia en servidores web, en Internet, con servicios como los que se encarga de ofrecer **Google Apps**. Pero ésta no parece ser la mejor alternativa para firmas de grandes dimensiones, que deben cumplir con normas de seguridad, detalles de juicios en algunos casos, backups históricos, y otras reglas. Todo esto podemos obtenerlo con motores de correo como Exchange, Thunderbird y otros. Con el paso del tiempo, la estructura de Exchange fue evolucionando, y hoy en día tenemos varios servidores cumpliendo distintos roles dentro de la infraestructura.

Estos servidores antiguos tenían todos los roles juntos. Es decir, había un servidor con una carga enorme en cada ubicación de la infraestructura de Exchange. Si se rompía alguno, nos quedábamos sin correo, y era muy difícil volver a su estado original debido a que su base de datos era difícil de recuperar. Hoy se utilizan bases de datos relacionales mucho más eficaces, como Microsoft Server.

Vimos la consola de Exchange 2007 en el **Capítulo 1**. En ella podemos tener todas las direcciones de mail, la configuración de la organización y la del servidor. También hay herramientas muy útiles para la administración, que nos permiten ver las colas de mensajes, seguir la ruta de ciertos mails, recuperar la base de datos, y otras.

CMS

Se trata de sistemas de gestión de contenidos. Ofrecen interfaces web para generar sitios; compartir datos, archivos e informes; generar colaboración y realizar todo tipo de interacción entre los empleados de la empresa. Permiten separar el contenido del diseño y, así, modificar y modernizar los ambientes de trabajo. Son utilizados para la generación rápida de sitios web.

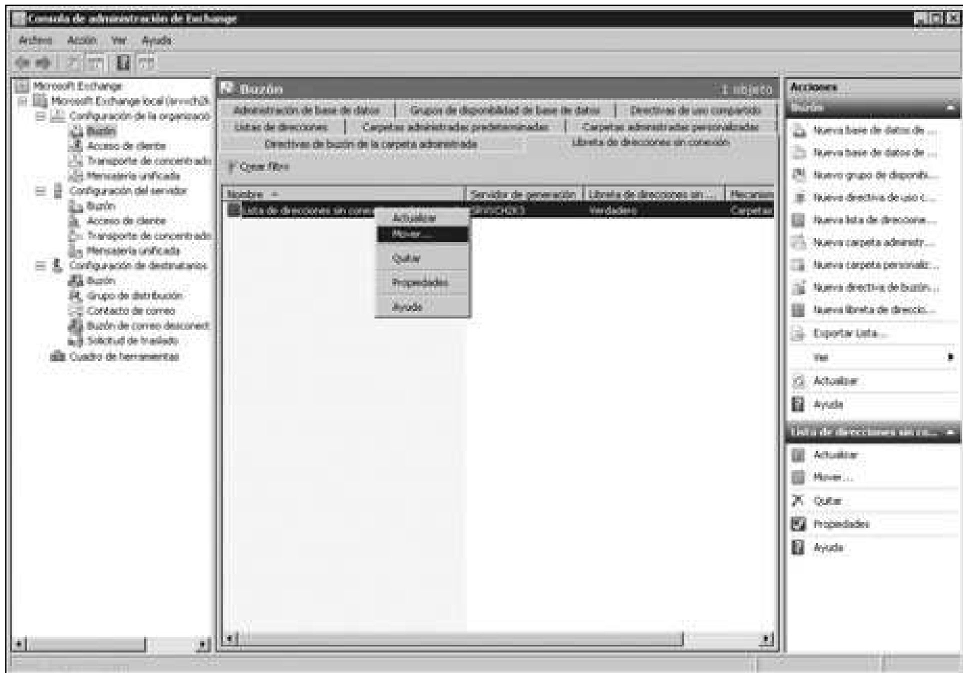


***Figura 6.** Los tres grandes grupos de configuraciones que trae actualmente el programa Exchange, de Microsoft.*

Aplicaciones de seguridad

Existe un gran cantidad de aplicaciones de seguridad en la red. El tema es muy amplio, y generalmente, tiene que ver con accesos, auditorías, permisos e informes. A continuación, nos encargaremos de describir en detalle la seguridad de las computadoras de escritorio, de los usuarios y de los servidores.

La PC de escritorio o servidor en la red debe tener instalado un cliente del antivirus corporativo; ésta es una regla primordial en cualquier organización. Este tipo de antivirus suele regularse mediante reglas corporativas y restricciones preestablecidas desde su instalación. Los clientes se conectan siempre contra un servidor central, que contiene estas reglas y actualizaciones de definiciones de virus. Podemos armar distintas políticas de administración que manejen distintos grupos de objetos; por ejemplo, una para PCs de escritorio, una para PCs portátiles y otra para servidores. Luego, también desde la consola principal, podremos obtener informes, reinstalar clientes, definir nuevas reglas, y más. En general, estos antivirus tienen un firewall integrado para el cliente y un motor de antispyware.

Otro nivel de seguridad más masivo es el firewall físico entre las redes, en donde el departamento de seguridad tiene pleno control. Éste ya es un hardware específico que cumple esta función, mucho más poderoso que un firewall de escritorio. Sólo debemos abrir los puertos que se usen, y mantener cerrados los demás. En la

navegación web sobre el proxy, también podemos tener otro tipo de firewall, como el **Isa Server** de Microsoft, para establecer reglas de navegación por Internet, bloquear páginas y aplicaciones que no aportan al trabajo diario de la empresa. Su última versión fue la lanzada en 2006. Actualmente, esta herramienta no tiene más actualizaciones y fue reemplazada por **Microsoft Forefront**. La herramienta que reemplaza al ISA Server es **Microsoft Forefront Threat Management Gateway**.

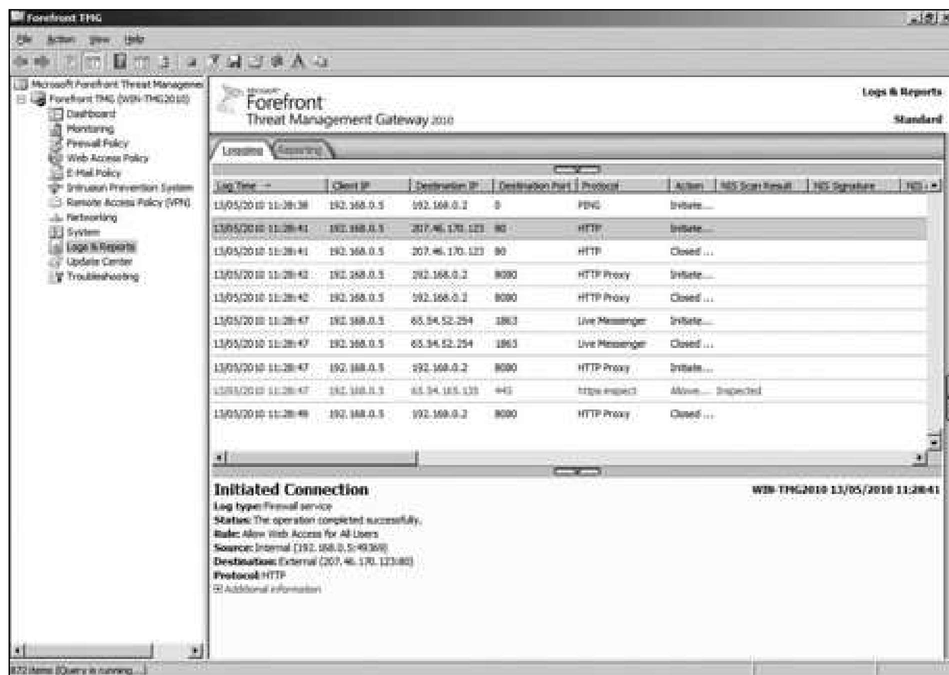


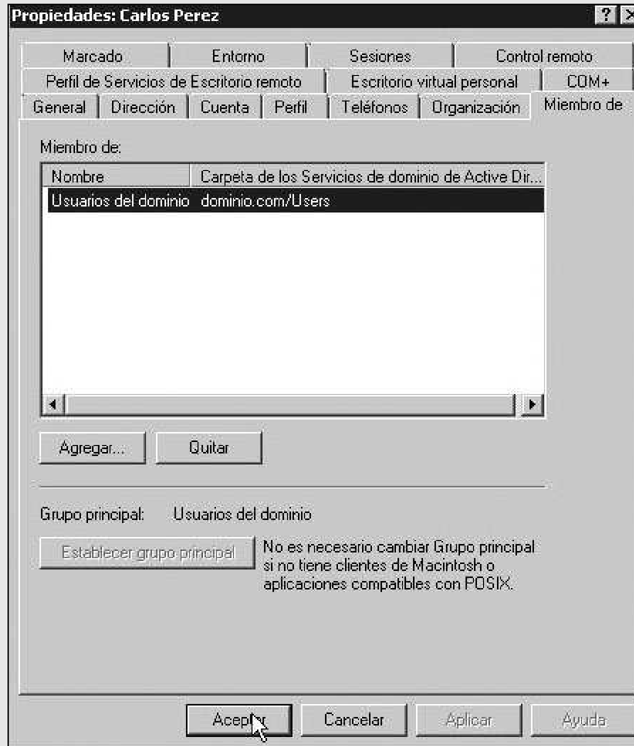
Figura 7. *Forefront TMG trae algunas otras opciones más de las presentes en su antecesor, pero sigue cumpliendo las mismas funciones: filtrado de tráfico de Internet, bloqueo de direcciones, etc.*

ISA Server nos permite bloquear o admitir páginas y configurar puertos para ciertas aplicaciones. Posee una jerarquía de reglas que los hosts seguirán cada vez que quieran entrar en un sitio web. También podremos configurar por qué conexión brindar el servicio, dado que es posible tener varios proveedores de Internet. Tendremos algunas herramientas como la de escaneo de cierta IP para una máquina, destinada a saber por qué falla alguna web a la que no se pueda acceder.

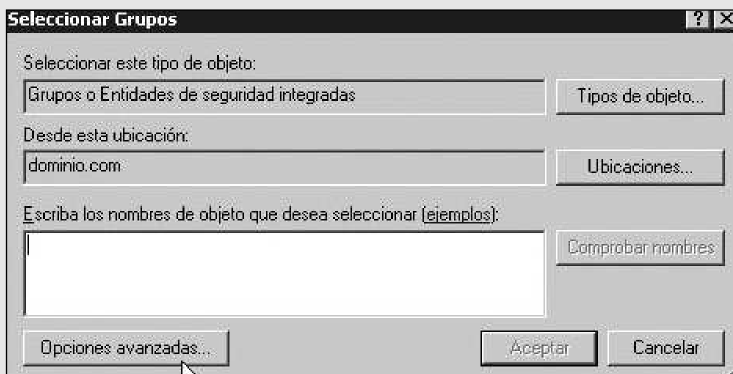
Active Directory también es una gran aplicación de seguridad. En ella se definen grupos de seguridad que tienen como miembros a los usuarios de la red; en algunos casos, también pueden tener equipos. Con estos grupos administramos grandes cantidades de usuarios al mismo tiempo. Por ejemplo, para dar permisos de escritura en una carpeta de un file server, podemos agregar de a un usuario o, directamente, añadir un grupo de seguridad creado previamente en Active Directory.

Agregar un grupo a un usuario — PASO A PASO

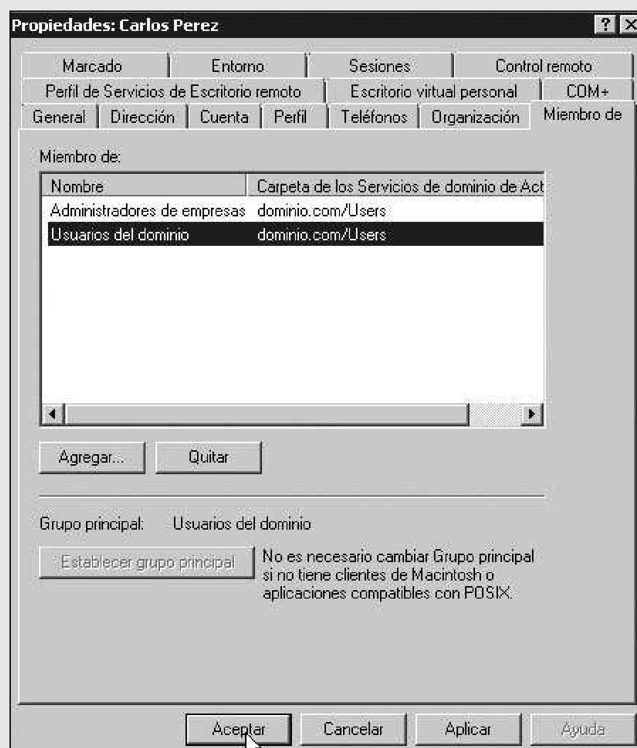
1 Abra la consola de **Usuarios y equipos de Active Directory** desde las **Herramientas administrativas** del menú **Inicio**. Haga doble clic en el usuario que desea modificar y diríjase a la solapa **Miembro de**.



2 Oprima el botón **Agregar** y escriba el nombre del grupo; si no lo recuerda, búsquelo presionando el botón **Comprobar nombres**.



▶ 3 Para continuar, haga clic en el botón llamado **Aceptar** y oprima otra vez **Aceptar** para cerrar la ventana de propiedades del usuario.



En Active Directory también podemos manejar los permisos para mandar mails en nombre de otra persona o en nombre de un grupo, utilizando otra cuenta de correo. Es posible administrar el tamaño de las casillas de correo y dar permisos de Exchange si tenemos extendida nuestra base de datos.

Herramientas para monitorear equipos

Es importante tener en cuenta que el monitoreo de los equipos de la red es relevante dentro de nuestras tareas diarias; es más, es una de las acciones primordiales para conseguir nuestro principal objetivo. Por esta razón será necesario que maximicemos el tiempo de respuesta para que un servicio quede funcionando la mayor cantidad posible de días. Para esta tarea existen diversas aplicaciones que pueden ayudarnos a monitorear los equipos. Algunas de ellas son **Operation Manager**, de Microsoft; **OpManager**, de la empresa Manage Engine (muy recomendada), y **Nagios**, la más utilizada por tener licencia GPL.

Nagios se instala en un servidor UNIX o Linux, mientras que Operation Manager y OpManager se emplean en ambientes Windows. Básicamente, todas realizan las mismas tareas: consultan por red los equipos cada tres o cuatro minutos para saber si están en línea; chequean los servicios y estados de memoria, de discos, de uso de CPU, etc.; y revisan cualquier tipo de servidor y cualquier switch, router o elemento en la red. Con estas aplicaciones, podemos administrar perfiles de alarmas, grupos de personas a quienes avisar, ya que envían e-mails y mensajes a los celulares. También, algunas aplicaciones de monitoreo pueden programarse para realizar alguna tarea en caso de que haya una alarma.

El monitoreo de los equipos es necesario y debe ser bien administrado. No sirve que la aplicación de monitoreo nos mande mails innecesarios o nos llene la casilla de mensajes: debemos administrar nosotros nuestra bandeja de entrada para poder distinguir lo que es realmente importante. Por ejemplo, saber que el disco **C:** de cierto equipo se está quedando sin espacio es menos preocupante que saber que el mismo equipo no responde. Para esto, debemos configurar reglas en Outlook que nos permitan obtener alarmas sonoras ante las caídas de los servidores o que nos avisen mediante un pop-up que veremos fácilmente. También hay otras reglas que indican eliminar automáticamente de la bandeja los datos menos preocupantes.



Figura 8. *Un ejemplo de lo que nos ofrece la consola de OpManager: estado de los equipos, detalles de la alarma, vistas, y muchas cosas más.*

Herramientas de colaboración

Estas herramientas son primordiales para lograr una buena comunicación empresarial. El uso de chat interno entre los usuarios de la red es cotidiano y fue consolidando su existencia gracias a Internet. Hoy en día, es un recurso de comunicación muy poderoso. Una aplicación de este tipo es **Communicator** (OCS), de la firma Microsoft. Esta herramienta es una versión avanzada del famoso **Messenger**, y se integra con **Live Meeting** y Outlook para dar una solución integral de conferencias en las cuales podremos compartir nuestra pantalla, y conversar con audio y video entre todos los participantes. También permite realizar llamadas a teléfonos de línea empleando protocolos de voz sobre IP. Se trata de una gran solución que poco a poco está evolucionando en la actualidad.

Algunas otras herramientas de colaboración son los **wikis** o **blogs**. En ellos podemos consolidar los conocimientos del grupo y guardarlos para futuras consultas. **SharePoint** es una herramienta moderna. Se trata de una aplicación que nos permite crear una intranet, un directorio de usuarios, un blog, compartir documentos y correos, etc. Se integra con OCS, Live Meeting y Outlook, así como también con otras herramientas de Microsoft. Posee un motor de búsqueda y permite administrar de manera eficiente toda la seguridad en la intranet. SharePoint no es más que un **CMS** (*Content Management System*, o sistema de manejo de contenidos). Otros CMS que podemos utilizar son **Joomla**, **WordPress** o **Drupal**; este último es muy conocido y utilizado por los usuarios, ya que es gratuito.

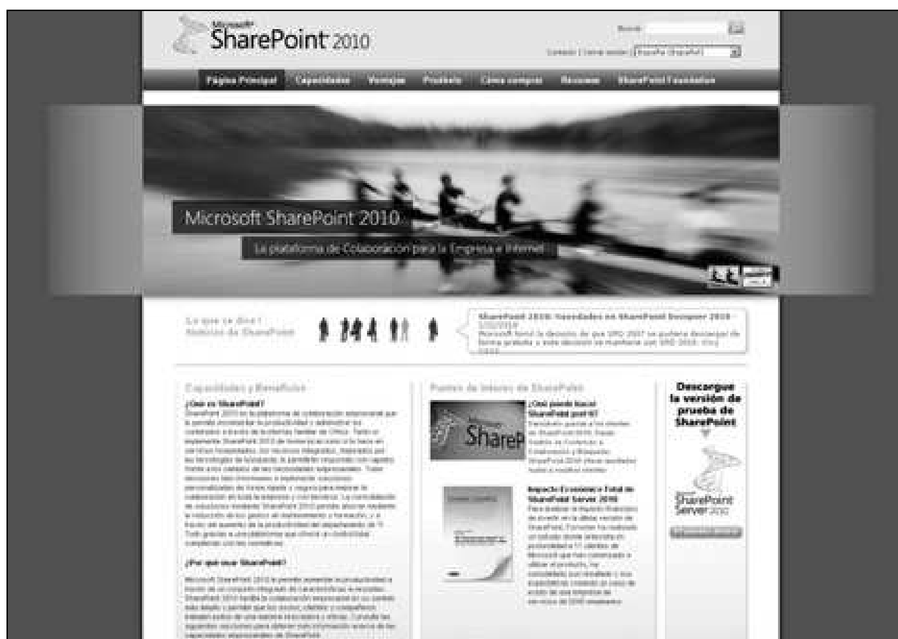


Figura 9. *El sitio oficial de SharePoint está realizado con la propia herramienta, también conocida como MOSS (Microsoft Office SharePoint Server).*

HERRAMIENTAS PARA EL ADMINISTRADOR

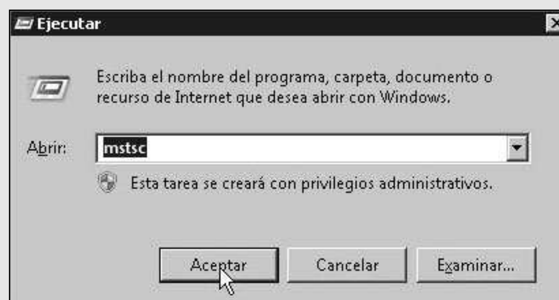
Luego de conocer y entender algunas aplicaciones que debemos brindar a nuestros usuarios en la red, detallaremos ciertas herramientas que utilizaremos para ofrecer un mejor servicio. Todas ellas son prácticas y necesarias, y nos ayudarán a no molestar el trabajo diario del personal accediendo remotamente a sus máquinas y, también, a ver detalles de servidores sin ocupar una sesión en el equipo. Por último, conoceremos paneles de control e informes que nos facilitarán la administración.

Accesos remotos

Los accesos remotos nos dan velocidad en la administración de los equipos. Los hay de varios tipos, y todos cumplen la función de accionar un equipo sin estar al lado de él físicamente. De este modo, podremos conectarnos desde dentro de la compañía o a través de Internet mediante una conexión **VPN**. Por ejemplo, estando dentro de la empresa, podemos conectarnos a un servidor como si fuese nuestro equipo de escritorio mediante la herramienta **Remote Desktop**, de Windows. Este programa nos permite tener dos sesiones por servidor y una más por consola. La sesión de consola es la que siempre está activa, y permite dejar aplicaciones ejecutándose en los servidores con algún usuario en particular, instalar parches, u otras acciones, y así poder loguearnos con otro usuario para efectuar otro trabajo. Para hacer esto, usamos una de las otras dos sesiones que nos da el servidor.
Remote Desktop también nos permite conectarnos a equipos de escritorio, con la diferencia de que, en estos últimos, sólo habrá una sesión activa, llamada sesión de consola. Si el usuario está utilizando la máquina y nos conectamos, cerraremos la sesión activa. A continuación, veremos cómo iniciar un acceso remoto.

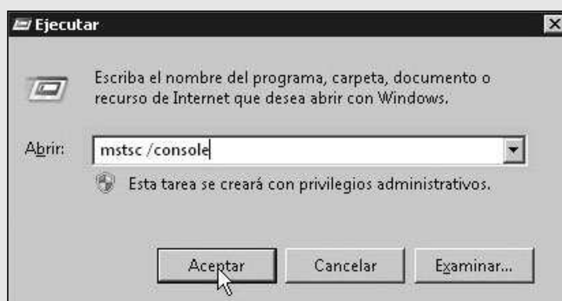
■ Ingresar a Remote Desktop — PASO A PASO

1 Vaya al menú **Inicio** y, en **Ejecutar**, escriba **mstsc**. En la ventana que se abre, ingrese el nombre del equipo al que quiere conectarse y oprima el botón **Aceptar**.

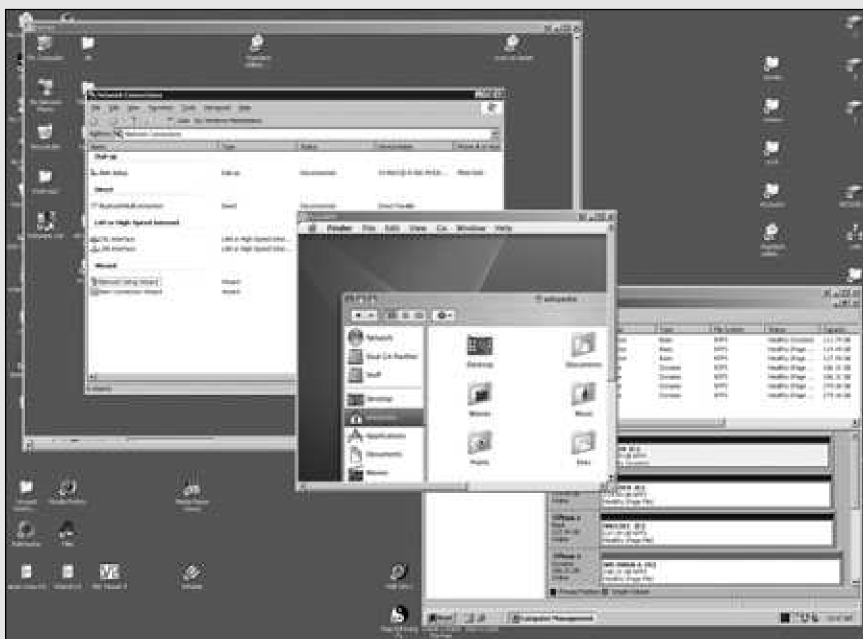


▶

2 Para abrir en modo consola, vaya al menú **Inicio** pero escriba **mstsc /console** o **mtsc / admin** en Windows 7. Luego, escriba el nombre del equipo para conectarse.



3 Abra más de una ventana y trabaje en más de un lugar al mismo tiempo, repitiendo los pasos anteriores.



Para acceder, previamente necesitamos dar permisos de acceso remoto. Para otorgar estos permisos a un equipo, debemos ir a las propiedades de **Mi PC**, allí dirigirnos a la solapa **Acceso remoto** y habilitar la opción adecuada. Otro modo de conectarnos a un equipo para manejar su escritorio como si fuera el nuestro es mediante algunas herramientas privadas, como **DameWare**. La diferencia con Remote Desktop, de Windows, es que estas últimas instalan un cliente en el equipo por conectar.

Otra posibilidad para acceder en forma remota a un equipo es desde las consolas en los centros de cómputos. Estas consolas suelen tener una dirección IP con la cual podemos acceder a ellas como si estuviésemos allí. El refresco de pantalla es mucho más lento, pero podemos ver hasta cuando se reinicia el equipo. Es muy importante tenerlas configuradas, porque nos permiten acceder igual si el equipo tiene problemas de red, ya que transmiten la información de nuestros periféricos como si fueran los propios de la consola.



***Figura 10.** La consola IP se conecta a todos los equipos en el centro de cómputos. Está físicamente allí; nosotros accedemos por red y, así, a todos los equipos conectados a ella.*

Otro tipo de acceso remoto es mediante la consola **MMC**. Con esta herramienta, por ejemplo, podemos conectarnos en forma remota a los servicios de un equipo que está en otro lugar. También podemos conectarnos a un **controlador de dominio** (*domain controller*) con el fin de administrar un DHCP o un DNS. Las posibilidades son infinitas. Entonces, no es necesario entrar e identificarse en los equipos de la red para hacer todas las tareas, sino que podemos utilizar los recursos de nuestra PC para hacerlo.
Otra opción para acceder remotamente es usando OCS. Con esta herramienta, el usuario puede compartirnos su escritorio y darnos permisos para manejar los periféricos como si fueran nuestros. Más adelante, en el **Capítulo 4**, veremos otra manera de conectarnos a un equipo en forma remota, pero ya desde un ambiente virtual.

Paneles de control

Los **paneles de control** permiten tener a nuestra disposición la información sobre el estado de toda la organización. Por ejemplo, el panel de control del monitoreo de hardware nos deja ver rápidamente si hay una alarma en un equipo al distinguir un color rojo. Podemos ver la evolución de las alarmas en el tiempo, además de obtener datos de disponibilidad y uso. También existen paneles de control de **tickets**, mediante los cuales podemos manejar los distintos pedidos de los usuarios. Eso sí, debemos acordarnos de cerrar los tickets a medida que se cumplan las tareas.

Estos sistemas trabajan con *workflows* (flujos de trabajo) y son cada día más populares. Algunos se integran con la infraestructura y realizan tareas automáticamente. Por ejemplo, mediante un workflow de pedido de alta de usuario, el ticket tendrá cargados los datos necesarios, se regirá por ciertas aprobaciones que tendrán que hacer los responsables y, luego, podrá disparar un evento, un script o una aplicación que realice el alta en Active Directory, copie el perfil de permisos de algún otro usuario y le dé una dirección de e-mail. SharePoint nos permite realizar nuestros propios paneles de control con las variables que queramos. Éstas pueden alimentarse de distintos sistemas o de diferentes tareas de usuarios. Son verdaderamente útiles cuando precisamos realizar el seguimiento de una tarea crítica.

Otro panel de control que podemos encontrar es el de backups. Un ejemplo es la consola de **Veritas Netbackup**, que nos ofrece el estado de las cintas de backup para verificar si están o no en el robot de backup, si están llenas o corruptas. También nos brinda detalles sobre el estado de los robots y de los trabajos que fuimos configurando para que se realicen, es decir, backups que mandamos a hacer desde la consola a equipos remotos.

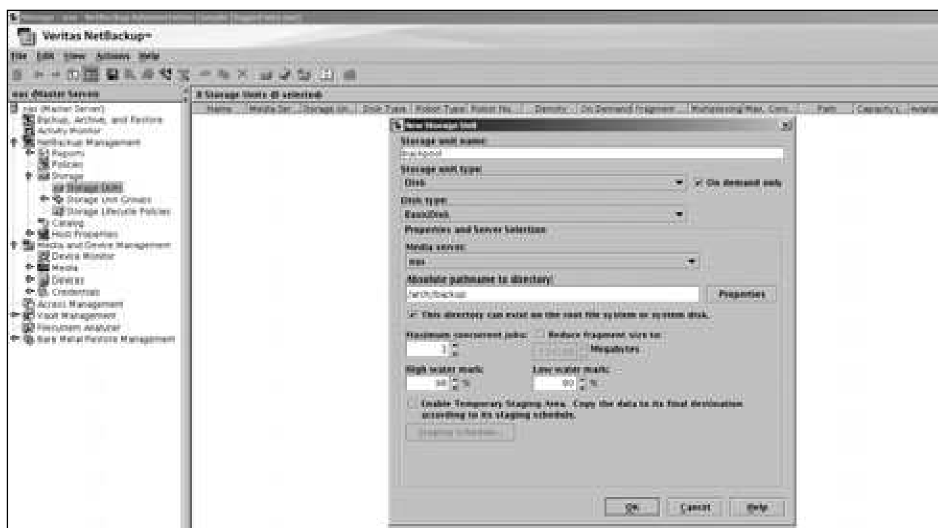


***Figura 11.** En forma online, veremos las cintas a nuestra disposición y el estado de los robots. También, el estado de los jobs y sus fallas.*

Informes

Los informes en la administración sirven para tomar decisiones. Podemos realizar informes de toda la información que necesitemos. Por ejemplo, pueden ser de avances semanales, de estado, de disponibilidad de servidores, de las bases de datos, del uso de discos, de estados del directorio de dominio, etc. En una buena administración, los informes tienen que ser periódicos, y deben ser chequeados y comparados a lo largo del tiempo para saber que las decisiones tomadas fueron certeras. Las decisiones pueden ser tomadas por nuestros jefes, en un nivel superior al de un administrador, pero si somos conscientes de nuestras funciones y nos gusta mostrar resultados, sabremos aprovecharlos. Debemos crearnos la rutina de efectuar los chequeos para saber dónde estamos parados y qué clase de tareas estamos realizando. Por ejemplo, podríamos decidir migrar una aplicación crítica si vemos que, al pasar los días, el uso de la CPU es cada vez mayor. A través de los informes, podemos prever situaciones catastróficas que pueden perjudicar nuestro objetivo de continuidad. Algunos informes importantes pueden ser conocer las capacidades de nuestra infraestructura de PCs para una futura migración, saber la antigüedad de nuestros equipos, saber qué software tenemos instalado y cuál tenemos licenciado, conocer los parches instalados y los que fallaron, etc. Más adelante, en el **Capítulo 5**, veremos que con System Center podremos tener una cantidad enorme de informes y hasta crear los nuestros.

… RESUMEN

Vimos en este capítulo la forma adecuada de instalar un servidor desde cero y brindar un servicio a los usuarios configurando la seguridad. Aprendimos que ésta se resalta con el uso de Active Directory y que la configuración de red tiene que ver en las tareas diarias. Conocimos conceptos nuevos y aplicaciones que vamos a utilizar en forma cotidiana. Ya estamos preparados para adentrarnos en el mundo de la seguridad exclusivamente, como paso intermedio para explotar las capacidades de nuestra empresa mediante el uso de VmWare y System Center Configuration Manager.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 ¿Qué es un rack y cuáles son las normas que los rigen?

2 ¿Cómo se conforma una dirección IP?

3 Describa las clases de IP que existen.

4 ¿Qué es un RAID?

5 ¿Qué niveles de RAID existen?

6 ¿Por qué es tan importante el correo electrónico?

7 ¿Qué función cumple el monitoreo?

8 Mencione algunas de las opciones para ingresar en un equipo en forma remota.

9 ¿Para qué sirven los paneles de control?

10 Enumere distintos tipos de informes.

EJERCICIOS PRÁCTICOS

1 Realice un informe de todas las aplicaciones de seguridad en su red.

2 Configure una alarma con envío de e-mails.

3 Cree varios usuarios en la red.

4 Configure un RAID 1 en algún equipo de la red.

5 Configure una alarma a un celular.

Seguridad corporativa

Ya conocemos los pasos necesarios para la instalación de servidores, y vimos algunas pautas para configurarlos en el dominio con Active Directory y con las herramientas que nombramos. Ahora veremos cómo darles seguridad física y lógica. Nuestra meta es que los equipos no sean dañados y no puedan ser modificados ni accedidos sin los permisos correspondientes.

POLÍTICAS DE SEGURIDAD

La aplicación de políticas de seguridad nos ayudará a tener nuestra infraestructura controlada y con configuraciones estándar. Debemos tener en cuenta que esta práctica se encarga de complementar la seguridad brindada por las aplicaciones antivirus y firewalls, pero es igualmente necesaria. Las políticas tienen una gran variedad de configuraciones para los servidores y los usuarios. Definiremos qué son, y veremos cómo administrarlas, aplicarlas y las nuevas características que podemos encontrar en un dominio con Windows Server 2008.

Qué son y cómo se aplican las políticas de seguridad

Las políticas de seguridad son reglas establecidas para el dominio de nuestra empresa. Existen políticas de usuarios y de máquinas. Las primeras restringen las acciones de los usuarios una vez que ingresan en la red; por ejemplo, podemos evitar que se ejecuten ciertos programas en los equipos y realizar muchas otras configuraciones.
Al aplicar políticas de máquinas, tenemos la opción de estandarizar las propiedades de las PCs de escritorio y los servidores para que tengan una configuración general única; es decir que cualquier usuario que use la máquina tendrá las mismas configuraciones. Por ejemplo, podríamos acceder a realizar la modificación de algunos servicios para que queden funcionando en forma automática, o también instalar un parche o aplicación al iniciar el sistema, además de cambiar los usuarios del equipo para incluir usuarios del dominio, etc. En muchos casos, deberemos crear estas reglas por pedido de los departamentos de Seguridad o de Recursos Humanos, pero es importante mencionar que una gran parte de ellas son establecidas para hacer funcionar algún sistema de la empresa en particular.
Utilizamos la herramienta denominada **GPMC** (*Group Policy Management Console*) de Microsoft para efectuar esta tarea. Debemos saber que no viene instalada en el sistema operativo por defecto, sino que tendremos que realizar los pasos correspondientes para agregarla. En Windows 2003 Server podemos bajarla del sitio oficial de Microsoft e instalarla en el sistema operativo; para Windows 2008 Server veremos la manera de agregarla paso a paso, como una característica nueva.

POLÍTICAS

Las políticas son reglas que impone la compañía a sus empleados para que utilicen el capital de la empresa en forma correcta, ya que restringen accesos de seguridad, configuraciones e instalaciones de programas indebidos. Active Directory nos permite crear directorios de dominios en los cuales administraremos toda nuestra infraestructura.

Instalar la consola GPMC en Windows Server 2008 — PASO A PASO

1 Conéctese al equipo que sea controlador de dominio (Active Directory), vaya al botón **Inicio** y abra el **Panel de control**. Ingrese en la opción **Activar o desactivar las características de Windows**.



2 Para continuar, oprima el botón derecho del mouse sobre la opción llamada **Características** del árbol y elija **Agregar características**.



▶

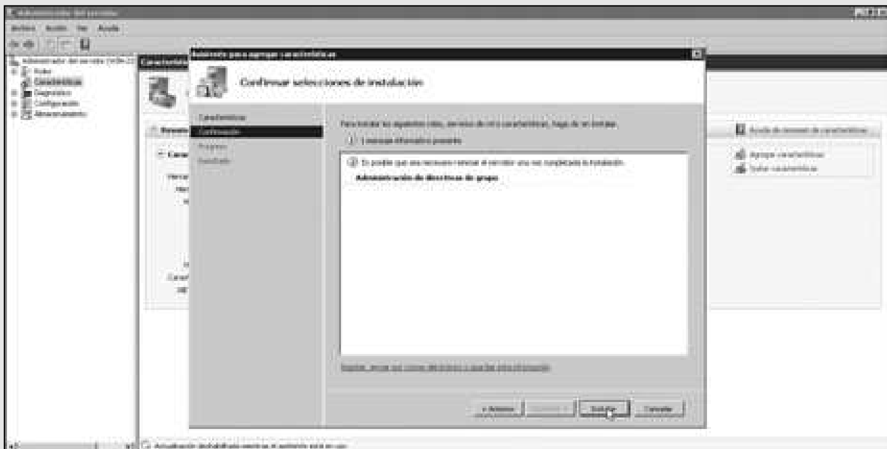
MICROSOFT SECURITY ADVISORY

Éste es un sistema de alertas de Microsoft que nos avisa de manera urgente cualquier novedad sobre vulnerabilidades y parches. En general, nos informa por e-mail, pero también tiene presencia en distintas redes sociales. Proporciona boletines diarios, asesoramientos, herramientas, orientación y recursos de la comunidad. **www.microsoft.com/technet/security/advisory**

3 Marque la opción **Administración de directivas de grupo** para agregar la nueva función que le permitirá administrar las políticas del dominio.



4 Oprima el botón **Instalar** para comenzar la instalación y espere unos minutos.



NETLOGON

Es una carpeta que se publica en el controlador de dominio de Active Directory cuando se lo instala, y por lo tanto, pertenece al dominio correspondiente. A ella pueden acceder todas las máquinas de la red y todos los usuarios. Lo harán con permisos de sólo lectura; los de modificación los tendremos nosotros, los administradores.

▶
5 Luego, compruebe que la instalación se realizó correctamente expandiendo el árbol debajo de **Característica/Administración de directivas de grupo**.



La consola conocida como GPMC se conectará a un controlador de dominio para mostrar la configuración del dominio Active Directory. Podemos ver un árbol, similar al de la herramienta denominada **Usuarios y equipos**, pero podremos darnos cuenta de que presenta algunas diferencias, ya que sólo se muestran las OU y las políticas aplicadas a cada una de ellas; por lo tanto, no será posible que veamos los objetos que se encuentran asociados a cada una.



Figura 1. *En la consola se distinguen una sección para generar búsquedas, otra para ver dónde están aplicadas las políticas, y una tercera que es el repositorio en donde se crean y se administran.*

Las políticas se aplicarán a todos los objetos que estén en la OU configurada. Por ejemplo, la OU **Argentina** contiene otra OU llamada **Computadoras**. A todos los objetos que tengamos en la OU **Argentina** se les aplicará la política **Default Domain Policy**, al igual que en la OU **Computadoras**, ya que las políticas se heredan. Decimos que las políticas están **conectadas** a las OU porque hay una carpeta especial que es el repositorio en donde se crean; luego se generan accesos directos a las OU para configurar las políticas en un determinado lugar del dominio. La carpeta se denomina **Objetos de directiva de grupo**. Una vez creada una política, se puede conectar o desconectar de distintas OU que necesitemos. Las políticas aplicadas a una máquina pueden chequearse desde la línea de comandos de la siguiente manera:

```
C:\>GPRESULT /R
```

Este comando muestra un listado con las configuraciones de políticas de cada máquina y las configuraciones de políticas de usuario que tenga la PC o el servidor en donde se ejecute. Es muy importante tenerlo en cuenta para comprobar la aplicación certera de las políticas. En ciertos casos, deberemos reiniciar el equipo para lograrlo. También podemos forzarlas a actualizarse usando el siguiente comando:

```
C:\>GPUPDATE
```

De todos modos, si existen políticas que necesitan un reinicio, el comando pedirá hacerlo en el momento. Es conveniente agregar el opcional **–f** para forzar el reinicio. Si estamos en duda, siempre debemos reiniciar.

Ejemplo de políticas corporativas

Existen políticas para configurar cualquier aspecto del uso de una máquina o servidor. Encontraremos muchos sitios en Internet con recomendaciones y detalles sobre cada configuración. Vamos a nombrar algunas de ellas y veremos un ejemplo práctico de cómo conectar una política a una OU.

Debemos tener en cuenta que si bien hay muchas políticas, las más utilizadas son, por ejemplo, establecer normas de longitud y detalles en la creación de contraseñas, deshabilitar o habilitar ciertos servicios que funcionan en el sistema operativo, iniciar una aplicación en forma automática luego de que el usuario acceda al sistema o instalar un parche de Windows o algún software.

A continuación, aprenderemos a publicar un paquete de software para todas las máquinas de la red y a configurarlo para que se instale al iniciar el sistema mediante una política de seguridad. En el Netlogon podemos publicar scripts y paquetes

de instalación para que sean accedidos por cualquier usuario de la red. Si existe más de un controlador de dominio que pertenezca al mismo dominio, esta carpeta se replicará con cada cambio que se haga, al igual que cualquier configuración que realicemos en Active Directory. Para acceder al Netlogon y copiar un archivo, sólo será necesario que escribamos el comando **\\nombredominio.com\netlgon** en el menú **Inicio** del sistema operativo, desde la opción denominada **Ejecutar**. Podremos darnos cuenta de que se abrirá la carpeta correspondiente al controlador de dominio adecuado. Luego de realizar esta tarea, debemos proceder a crear una carpeta para la aplicación y, posteriormente, copiar el ejecutable.

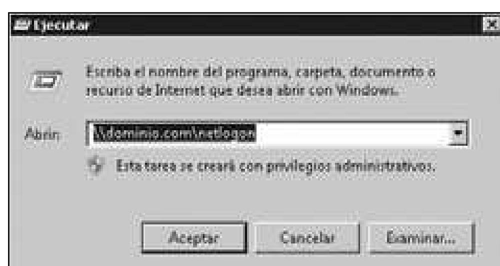
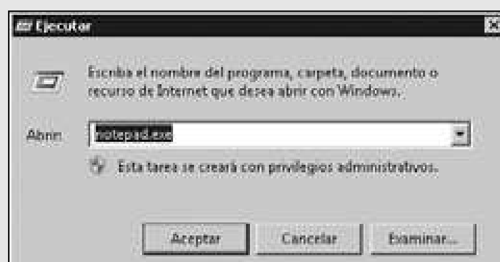


***Figura 2.** Una vez que creamos la carpeta, copiamos el instalador de la aplicación deseada en ella. Nos quedará una ruta parecida a **\\nombredominio.com\netlogon\carpetaapli\aplicacion.exe**.*

El paquete de instalación podrá ser leído por cualquier usuario de la red. Así como este paquete, podremos copiar el de cualquier programa. Para continuar, veremos cómo configurar la instalación del paquete para todas las máquinas. Debemos crear un script de instalación, guardarlo en la misma carpeta del Netlogon y, como último paso, crear una política que corra el script al inicio del sistema desde la consola GPMC. El script debe crearse utilizando un editor de textos.

■ Crear una política y conectarla a una OU — PASO A PASO

1 Vaya al menú **Inicio/Ejecutar** y escriba el comando **notepad.exe**, para abrir el editor de texto.



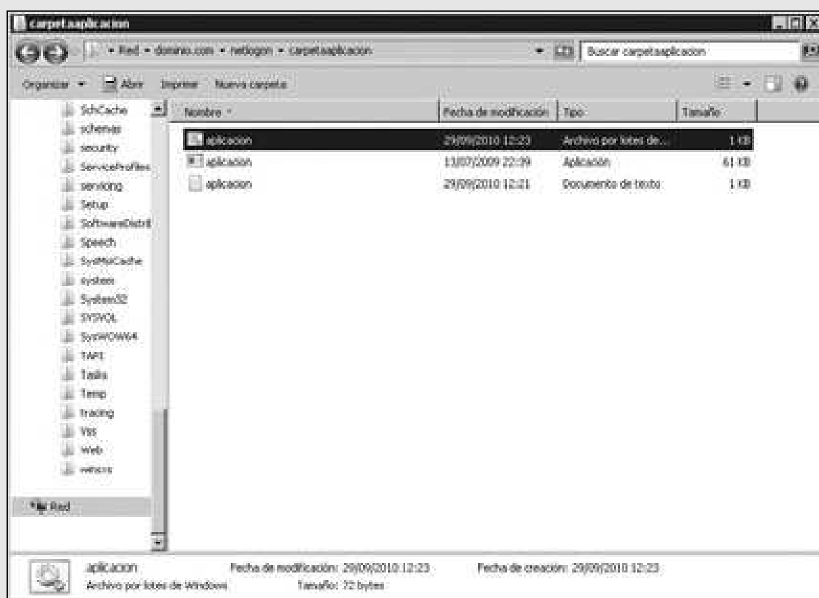
▶

▶

2 Para continuar, será necesario que escriba el siguiente texto en el editor de notas del sistema operativo: **@echo off**. Debe tener en cuenta la necesidad de dejar un renglón. Luego escriba (para el ejemplo que mencionamos más arriba): **\\nombredominio.com\netlogon\carpetaaplicacion\aplicacion.exe**. Por último, guarde el archivo utilizando el menú adecuado.

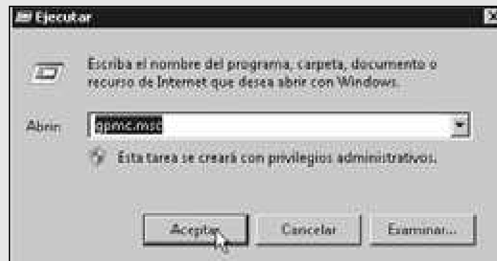


3 Renombre el archivo para cambiar su extensión **.TXT** por **.BAT** o guárdelo desde el editor de notas con esa extensión. A continuación, muévalo para ubicarlo en la carpeta de la aplicación en el **Netlogon**.

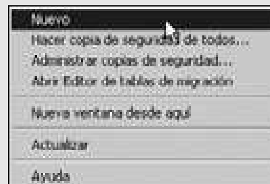


▶

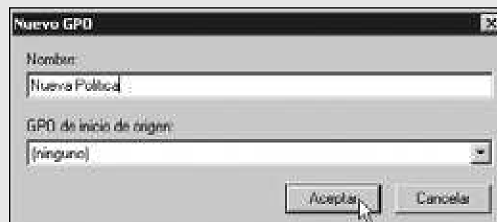
4 Vaya a **Inicio/Ejecutar**. Escriba **gpmc.msc** para abrir la consola de comandos.



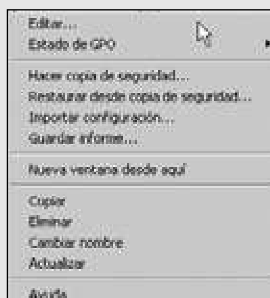
5 Posiciónese en **Objetos de directiva de grupo** y elija la opción **Nuevo**.



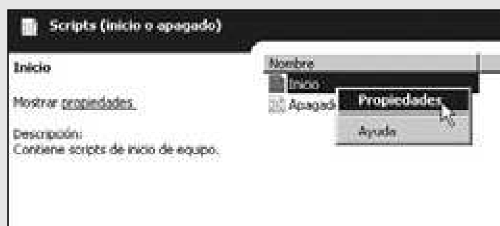
6 Escriba un nombre para la política y oprima el botón **Aceptar**. Deje la lista desplegable de abajo como está por defecto.



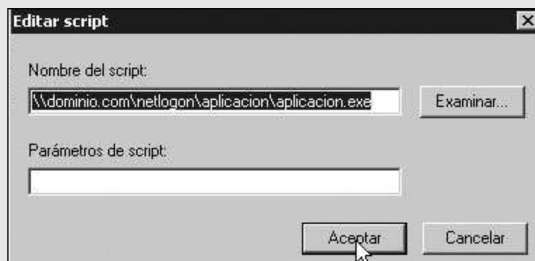
7 Vaya a la política recién creada y posteriormente haga clic con el botón derecho del mouse en ella. Elija **Editar** para poder configurarla.



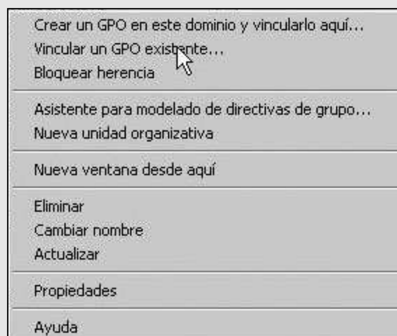
8 A continuación, expanda el árbol de **Configuración del equipo** y luego diríjase a la sección denominada **Configuración de Windows**. Expanda nuevamente el árbol y elija la opción llamada **Scripts**. En el lado derecho de la pantalla haga clic derecho sobre **Inicio** y escoja la opción **Propiedades**.



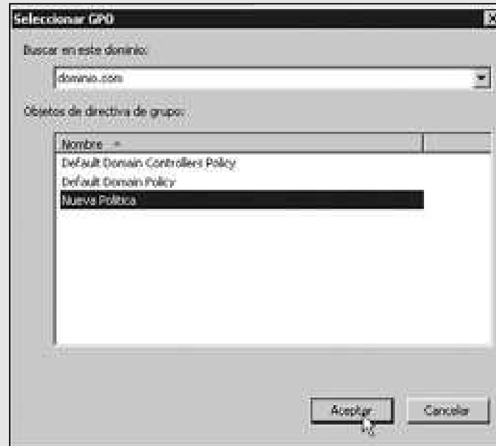
9 Para continuar, oprima el botón denominado **Agregar** y posteriormente escribir la ruta del script; en este caso deberá copiar la que se muestra a continuación: **\\dominio.com\netlogon\aplicacion\aplicacion.bat**.



10 En este paso deberá oprimir el botón **Aceptar**, luego de lo cual tendrá que cerrar la pantalla de edición. En la consola posiciónese donde quiera conectar la política. Para todas las computadoras de escritorio, ubíquese en la OU denominada **Computadoras**. Para continuar, haga clic con el botón derecho del mouse y elija la opción **Vincular un GPO existente**.



▶ 11 Elija la nueva política antes creada del listado que figura en pantalla y finalmente haga clic sobre el botón llamado **Aceptar**.



Una vez que se reinicie el sistema, se comenzará a instalar la aplicación con las credenciales de un usuario administrador, se llamará al script y se ejecutará en forma oculta. En todos los sistemas operativos Windows este tipo de tareas se realiza con el **usuario de sistema**. Se trata de un usuario especial con privilegios de administración que sólo puede ser manejado por el mismo sistema operativo. Otro tipo de política muy utilizada, y un poco distinta de la empleada en los procedimientos anteriores, es configurar todos los servicios de los equipos de la empresa. Para hacerlo, debemos crear una política nueva que aplicaremos a todas las máquinas. Abrimos la política y la editamos, luego expandimos el árbol hasta la opción de servicios del sistema ubicada en **Configuración del equipo/Directivas/Configuración de Windows/Configuración de seguridad/Servicios del Sistema** y allí modificamos los que queremos configurar. Antes de cambiar la política, tenemos que probarla muy bien para que no haya problemas con la compatibilidad de distintos sistemas de la empresa.

Políticas avanzadas para Windows 7 y Windows Server 2008

Estuvimos aprendiendo cómo configurar algunas políticas de seguridad, la aplicación de otras es muy similar a las vistas anteriormente. Ahora conoceremos qué es lo nuevo que nos trae el directorio de dominio de Active Directory con **Windows Server 2008 R2**. El sistema operativo incluye algunos cambios y algunas ventajas con respecto a su antecesor, **Windows Server 2003**. Nombraremos los más destacados en cuanto a políticas de seguridad.

Antes, con Windows Server 2003, los scripts de las políticas de inicio de sistema utilizaban el lenguaje **vbscript**, y no podía emplearse Power Shell. Afortunadamente, ahora sí podemos usarlo, lo que nos otorga mayor flexibilidad y varias configuraciones que antes no podíamos aplicar. Este motor de scripts puede agregarse en equipos con Windows Server 2003 y así utilizarlo una vez que el sistema se inicia. De todos modos, no podemos configurar una política de inicio con él. Otro cambio importante es que tenemos la opción de restringir los diseños de las contraseñas para distintos tipos de usuarios. El diseño es la estructura que definimos para que una clave exista. Antes sólo podíamos tener un único diseño para todos los usuarios del dominio. Por ejemplo, podemos establecer la longitud que deberá tener, si hay que utilizar caracteres especiales, si debemos tener minúsculas y mayúsculas, etc. Con Windows Server 2008 podemos tener distintos tipos de usuarios y configurar restricciones acordes a cada uno. Puede servirnos, por ejemplo, si deseamos que las contraseñas de usuarios de alto nivel administrativo sean más seguras que las de un usuario común.

ACCESO A LOS CENTROS DE CÓMPUTOS

Si dejamos de lado la protección contra un incendio o brindamos total libertad en el acceso al centro de cómputos, estaremos en problemas tarde o temprano. A continuación haremos una descripción de los puntos importantes para tener en cuenta con respecto a la seguridad física. También, extendiendo la introducción del **Capítulo 2** a lo que es un plan de contingencias, detallaremos aún más sus características y explicaremos cómo crear uno.

Seguridad física en los centros de cómputos

La seguridad física es muy importante para la administración. El centro de cómputos es el lugar en donde se conectan los equipos servidores que nosotros administramos. Puede tener distintos tamaños según la cantidad de equipos que albergue. No sólo tiene equipos servidores, sino que también cuenta con varios elementos que se deben proteger. Tiene un piso técnico (piso flotante por debajo del cual se pasan los cables), racks, armarios, un equipo de control de temperatura, otro para control de energía y uno para controlar incendios.

Es preciso controlar el indicador de temperatura, ya que un equipo puede generar demasiado calor, más del soportable, y hasta alguno puede quemarse. Los racks son capaces de albergar servidores y switches, consolas para conectarse a los equipos y pacheras. Deben estar bien ventilados, refrigerados y ordenados para que todo funcione correctamente. No sólo tenemos servidores que resguardar, sino todo un grupo de elementos físicos que son muy importantes. Debemos protegerlos, entonces, contra

intrusos, desastres naturales, incendios, sabotajes, y otros factores. Necesitamos ser cuidadosos con el acceso de intrusos, porque puede haber un sabotaje a los servidores y, también, ataques mucho más graves.
Como administradores, podemos restringir el acceso de varias formas. Una es utilizar un lector de tarjetas magnéticas, un escáner de iris o de mano, o un simple guardia. También, contar con un sistema de cámaras como respaldo de la seguridad, que son fáciles de instalar y muy utilizadas actualmente. Los lectores de tarjetas y escáneres trabajan con un servidor y algunos dispositivos mecánicos ubicados en las puertas. El dispositivo lee la tarjeta, la huella, la palma de la mano o el iris, y manda la información hacia el servidor habilitante. Si ésta se encuentra cargada en la base de datos, el servidor envía una señal de apertura a la cerradura del centro de cómputos y habilita la entrada.



Figura 3. *Algunos centros de cómputos están fuertemente protegidos mediante grandes y pesadas puertas. Otros, en cambio, no dan demasiada importancia a la construcción y su seguridad.*

Otra amenaza importante son los incendios, que pueden originarse de varias maneras, motivo por el cual es necesario estar preparados. El piso, el techo y las paredes deben estar creados con materiales ignífugos y no tiene que haber ningún elemento inflamable dentro del centro. Es fundamental contar con algún equipo controlador de incendios en estado latente, generalmente, mediante polvo químico o dióxido de carbono. Como administradores, podemos adoptar como práctica la realización de un chequeo diario visual en el centro de cómputos, con el fin de verificar posibles alarmas en los servidores y equipos de electricidad, controlar la temperatura y mantener el orden. Los servidores traen indicadores que es necesario revisar, que nos dicen cuando una fuente falla, un disco está roto, una placa funciona mal, hay problemas con un cooler o memoria RAM, etc. Si no llevamos un control, podemos encontrarnos con un servidor fuera de línea sin saber cuál fue el origen del problema. Una buena práctica sería llenar un formulario diario, y hacerlo llegar a todos los administradores y responsables cada día. Si vamos más allá, podemos realizar un informe de inicio de jornada y otro al finalizar, que detalle los arreglos que se realizaron y los que quedaron por hacer. Algunos pasos para llevarlo a cabo son los siguientes:

- Al iniciar el día, imprimimos un formulario y vamos hasta el centro de cómputos. Anotamos todo el control en él.

All computers

111 Result(s)
(Download)

Show: 20

Add column Reset

1 ... 6

	Last inventory	Computer	Operating system	RAM(MB)	CPU(MHz)
	04/04/2007 14:48:44	W16753101AAB	Microsoft Windows 2000 Server	1024	2660
	04/04/2007 14:45:28	HICOM	Microsoft Windows XP Professional	512	1002
	04/04/2007 14:44:26	ST32635RB	Microsoft Windows XP Professional	1024	2793
	04/04/2007 14:43:22	ST209036AHE	Microsoft Windows XP Professional	1024	2793
	04/04/2007 14:36:38	W16753101AAG	Microsoft Windows 2000 Server	1280	1393
	04/04/2007 14:36:00	ST32481DEV	Microsoft Windows XP Professional	1024	2399
	04/04/2007 14:31:17	CAMEL-2K-DEV	Microsoft Windows 2000 Server	1024	2391
●	04/04/2007 14:31:02	PTRCM320	Microsoft Windows XP Professional	735	2392
	04/04/2007 14:28:43	AV-PMF-6-XP	Microsoft Windows XP Professional	512	2793
	04/04/2007 14:22:51	ST32443RR	Microsoft Windows XP Professional	1024	2399
	04/04/2007 14:20:40	ST32639EXT	Microsoft Windows XP Professional	1024	2792
	04/04/2007 14:19:09	LABO-AV-2K-01	Microsoft Windows 2000 Server	2040	2666
	04/04/2007 14:16:31	ST32455DP	Microsoft Windows XP Professional	1024	2399
●	04/04/2007 14:16:27	PT32536DEV	Microsoft Windows XP Professional	1024	2391
	04/04/2007 14:09:25	ST32611EXT	Microsoft Windows XP Professional	1024	2792
	04/04/2007 14:08:52	LABO-AV-2K-02	Microsoft Windows 2000 Server	2048	2666
	04/04/2007 14:05:59	W16753101AAI	Microsoft Windows 2000 Server	1024	2394
	04/04/2007 14:04:32	ST32528DEV	Microsoft Windows XP Professional	1024	2391
	04/04/2007 14:04:26	LABO-AV-NT-03	Microsoft Windows NT 4.0 Server	1280	666
●	04/04/2007 14:04:04	W16753101AAJ	Microsoft Windows 2000 Server	1024	2394

Figura 4. *Un informe de inventario de todos los servidores de la empresa es de gran utilidad. También podemos hacer un formulario especial para el chequeo diario.*

- Verificamos en primer lugar que no haya luces rojas en los servidores. Si las hay, abrimos el panel de luces y buscamos información que indique la causa.
- Comprobamos ahora que no haya luces naranjas en los servidores. Si las hay, buscamos otra vez las causas y completamos el formulario.
- Nos dirigimos al panel de control de electricidad y en él verificamos en forma cuidadosa que no haya ningún indicador encendido.



***Figura 5.** Tenemos que ser muy cuidadosos al manipular este tipo de paneles, ya que podemos quedarnos electrocutados o dejar sin luz a gran parte de la compañía.*

EQUIPOS DE REFRIGERACIÓN

Debemos tener en cuenta que los equipos de refrigeración se encargan de bajar la temperatura emitida por los servidores dentro de la sala del centro de cómputos y de esta forma la mantienen a unos 22° C. Un aspecto importante es que conservan un flujo constante de aire que circula desde el frente de los racks hacia la parte posterior.

- Vamos hasta el controlador de temperatura del centro de cómputos y verificamos que esté en 22 grados o por debajo de ese valor. También miramos atrás de los racks para hacer un testeo perceptivo en busca de focos de calor intensos.
- Entramos en la consola de monitoreo lógico y verificamos las alarmas del día. Completamos el formulario, lo digitalizamos y lo enviamos por mail a los responsables.

Figura 6. *El monitoreo lógico puede hacerse con varias herramientas, pero es importante dejar impreso un documento como historial del estado de los equipos.*

Plan de contingencias

Continuando con la introducción que hicimos en el **Capítulo 2**, detallaremos un poco más lo que es un plan de contingencias y qué aspectos debemos tener en cuenta. Básicamente, el plan de contingencias nos dice **qué hacer** en caso de que ocurra



DÓNDE CREAR EL CENTRO DE CÓMPUTOS

Las amenazas naturales no son tomadas en cuenta en muchas ocasiones, pero en caso de tener que planificar la instalación de un centro de cómputos, es preciso establecer una buena zona donde hacerlo, en prevención de algún posible desastre. Por ejemplo, no debería de estar en inmediaciones de productos inflamables ni en zonas de inundaciones o huracanes.

una situación no deseada. Tiene que contener todas las tareas que debemos realizar para que el centro de cómputos vuelva a su estado original y operativo. El plan contempla posibles incendios, catástrofes, cortes de luz, sabotajes, etc. La capacidad para recuperarse exitosamente de un desastre en un corto período es crucial para el negocio. Hay empresas que, al no tener un plan de contingencias, tardan años en recobrarse operativamente, con las correspondientes pérdidas económicas, del negocio y, posteriormente, quiebra.
Replicar el centro de cómputos es lo mejor que podemos hacer, siempre y cuando la réplica se encuentre en un lugar alejado, para que no sufra las mismas causas de desastre. Pero éste es un detalle de seguridad física; el plan de contingencias viene a decirnos los pasos que debemos seguir para que el cambio sea satisfactorio. Nos indica qué palanca mover, hacia dónde y el tiempo que tenemos para hacerlo. El plan de contingencias, generalmente, se extiende del plan general de la empresa. Indica las salidas de emergencia, la ubicación de los manuales de emergencia, los procedimientos por seguir, los responsables y los teléfonos a donde llamar. Podríamos hacerlo teniendo en cuenta los siguientes puntos:

- Pensar en los posibles desastres que pueden ocurrir e identificar los riesgos que la empresa afrontaría en caso de que sucediera alguno. Luego, evaluar las pérdidas económicas, y realizar estadísticas y gráficos.
- Aplicar los conocimientos sobre los sistemas de la empresa, y jerarquizar las aplicaciones en críticas y no críticas.
- Establecer los requerimientos de recuperación. Tomar nota de todo lo necesario y los pasos por seguir con cada sistema. Luego, generar documentación clara.
- Implementar el plan de contingencias, realizar pruebas y simulacros para verificar que los procedimientos son los indicados antes de que sea tarde.
- Difundir el plan de contingencias en la empresa mediante comunicaciones masivas e indicadores. Por último, será necesario planificar en detalle un mantenimiento y chequeo del plan cada cierto tiempo.

La ejecución y puesta a punto del plan de contingencias es responsabilidad nuestra y de toda la empresa. Por eso, debemos asegurarnos de que haya una buena



ESTADÍSTICAS DE DESASTRES

Se sabe que las causas más comunes de los desastres son el terrorismo, los incendios y los huracanes. Imaginemos por un instante perder todos los datos de la compañía para siempre o perder las comunicaciones de la empresa durante semanas. Debemos ser conscientes de estas posibles amenazas y actuar antes de que ocurran.

comunicación y de que cada empleado lo conozca. La continuidad del negocio depende de un buen plan de contingencias.



***Figura 7.** El análisis de un evento crítico de tal magnitud requiere de controles muy severos y coordinación de toda la empresa.*

NORMAS DE SEGURIDAD

En esta sección veremos normas que están en el mercado y nos permiten certificarnos en calidad (ISO9001), en seguridad (ISO27001) y en buenas prácticas (ISO20000). **ITIL** no es una certificación propiamente dicha, pero las empresas están aplicando los procedimientos descriptos como tal. Estas prácticas provienen del Reino Unido. A continuación, analizaremos las normas ISO20000 e ISO15000, que tienen una certificación valedera y se basan en procedimientos de ITIL.



SISTEMAS SGSI

El Sistema de Gestión de la Seguridad de la Información (SGSI) sirve para el diseño, la implantación y el mantenimiento de un conjunto de procesos tendientes a gestionar eficientemente la accesibilidad de la información, buscando asegurar confidencialidad, integridad y disponibilidad de los activos de información, a la vez que minimiza los riesgos de seguridad.

Normas ISSO 9001 y 27001

Las normas ISO 9001 y 27001 son estándares elaborados por la Organización Internacional para la Estandarización, una federación internacional de los institutos de normalización de 157 países; organización no gubernamental con sede en Ginebra (Suiza). Todos estos países, en consenso, estudian los estándares requeridos por el mercado sobre tecnología, productos, métodos de gestión, etc. El organismo no obliga a aplicar los estándares; esto es voluntario y sólo es obligatorio si en el país rige una legislación sobre su aplicación.
La norma ISO9001 especifica los requerimientos para un buen sistema de gestión de la calidad. Actualmente, existe la cuarta versión de la norma, publicada en el año 2008, razón por la cual se la llama, internacionalmente, ISO9001:2008.



***Figura 8.** Sello con el que debería contar nuestra empresa para ofrecer calidad en los productos. Nuestro sector también puede tener este sello para distinguirnos dentro de la organización y que los usuarios confíen más en los servicios brindados.*

Tanto esta norma como las otras, de las cuales hablaremos más adelante, pueden servir a la empresa para trabajar mejor o, en muchos casos, como parte de su plan de marketing. Algunas compañías sólo certifican determinados departamentos o productos específicos, y no, la organización en su integridad. Esto las ayuda a tener



ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)

Es un resumen de las buenas prácticas en la entrega de servicios de tecnologías de información (IT). Fueron desarrolladas en el año 1980 por la **Central Computer and Telecommunications Agency** (**CCTA**), del gobierno británico, como respuesta a la creciente demanda y falta de un estándar, lo que generaba duplicaciones de investigación y grandes gastos a las empresas.

mejores ventas con una buena campaña publicitaria, sin realizar el gran esfuerzo que implica certificar todos y cada uno de los procedimientos.
Pero nosotros tenemos que enfocarnos en lo que estas normas significan para la administración de servidores. La norma ISO9001 nos da una gran ayuda para mantener una guía de calidad en nuestro trabajo. Aplicarla hasta los límites que podamos hacerlo seguramente nos gratificará tarde o temprano.
La norma ISO9001:2008 se compone de ocho capítulos:

CAPÍTULO	DESCRIPCIÓN
I	Guías y descripciones generales
II	Normativas de referencia
III	Términos y definiciones
IV	Sistema de gestión
V	Responsabilidades de la Dirección
VI	Gestión de los recursos
VII	Realización del producto
VIII	Medición, análisis y mejora

Tabla 1. *Los ocho capítulos de los que se compone la norma ISO9001:2008.*

Aplicar la norma en la empresa es una carta de presentación al mundo, significa decirle que tenemos calidad en lo que hacemos. La aplicación nos otorga una mejora en toda la documentación, nos asegura que la información se actualice y sea efectiva, reduce los costos y disminuye la cantidad de procesos.
La norma 27001 gestiona la seguridad. Se basa en un Sistema de Gestión de la Seguridad de Información, también conocido como SGSI. Este sistema, bien implantado en una empresa, nos permitirá hacer un análisis de los requerimientos de la seguridad de nuestro entorno. Con ellos, podremos crear procedimientos de mantenimiento y puesta a punto, y aplicar controles para medir la eficacia de nuestro trabajo. La norma contempla cada uno de estos requisitos y nos ayuda a organizar todos los procedimientos. Todas estas acciones protegerán la empresa frente a amenazas y riesgos que puedan poner en peligro nuestros niveles de competitividad, rentabilidad y conformidad legal para alcanzar los objetivos planteados por la organización.



LIBROS Y VERSIONES DE ITIL

Su última versión, la tercera, fue publicada en 2007 con ciertas modificaciones. En las anteriores, las continuas modificaciones y actualizaciones dieron lugar a 31 libros para la versión I y 30 libros para la versión II. El grupo originario se propuso minimizar esta cantidad y, así, en la versión 3 de 2007 tenemos sólo 8 libros y uno complementario.

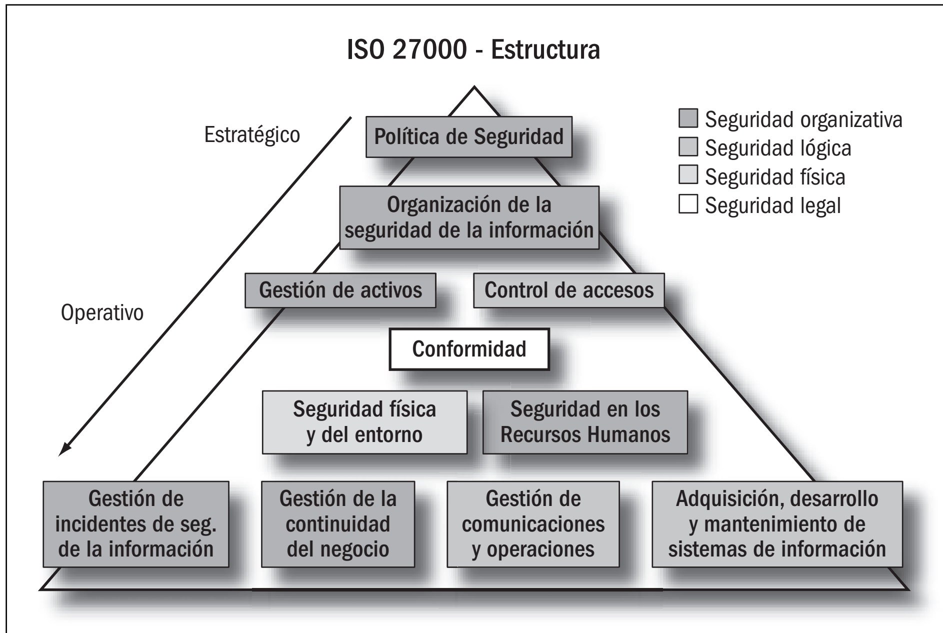


Figura 9. *Estructura en la que se basa la ISO 27001. Vemos los niveles estratégicos y operativos que debemos cumplir.*

Nuestro objetivo al aplicar esta norma tiene que ser asegurar la confidencialidad, integridad y disponibilidad de la información para nuestros empleados, clientes y cada persona que intervenga en el negocio. La aplicación no sólo expresa nuestras buenas prácticas en la materia, sino que también nos ayuda con ciertos requerimientos legales de nuestra legislación. Obviamente, la legislación dependerá del gobierno de cada país, pero a grandes rasgos, nos ayuda con leyes de protección de datos personales, de inspección y de control, y también en juicios, en los que casi siempre se solicitan datos históricos.

ITIL y la norma ISO20000

ITIL proviene del inglés *Information Technology Infrastructure Library*, biblioteca de infraestructuras de tecnologías de la información. Es un marco de referencia de mejores prácticas para gestionar operaciones y servicios de IT. Fue definido en los años 80 por el Reino Unido y es, sencillamente, el sentido común documentado a lo largo de los años de aprendizaje de gestores de departamentos de helpdesk de todas partes del mundo. ITIL no es un estándar; no existe una certificación ITIL, podemos obtenerla certificación de las normas ISO20000 o BS15000 que se basan en ITIL. Cualquier empresa puede implementar ITIL, pero es recomendable para aquellas que tengan más de cinco personas en el departamento de helpdesk. Fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la gestión de IT.

Los libros de la última versión son los siguientes:

1. Mejores prácticas para la provisión de servicio
2. Mejores prácticas para el soporte de servicio
3. Gestión de la infraestructura de IT
4. Gestión de la seguridad
5. Perspectiva de negocio
6. Gestión de aplicaciones
7. Gestión de activos de software
8. Planeando implementar la gestión de servicios
9. Implementación de ITIL a pequeña escala (complementario)

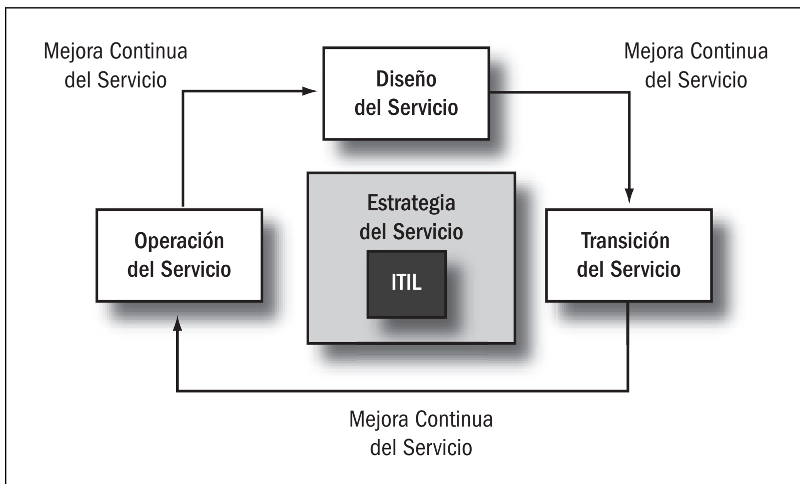


Figura 10. *Podemos observar el ciclo de vida de ITIL dentro de una empresa, que podría ser la nuestra.*

La ISO20000 fue publicada en diciembre del año 2005. Nos permite concentrarnos en una gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia. También controla la capacidad del sistema, los niveles de gestión necesarios cuando éste cambia, la asignación de presupuestos, y el control y la distribución del software.
Debemos tener en cuenta que la norma se divide en tres partes: la primera se encarga de realizar la definición de los requisitos necesarios para diseñar, implementar y mantener la gestión de servicios IT de una empresa; la segunda nos enseña cuáles son los mejores procedimientos para los procesos de gestión de servicios, las mejores prácticas codificadas según el mercado; y por último, la tercera parte es una guía sobre el alcance y la aplicabilidad de la norma correspondiente. En la primera, los requisitos pueden detallarse como se indica a continuación:

- Requisitos para un sistema de gestión
- Planificación e implantación de la gestión del servicio
- Planificación e implantación de servicios nuevos o cambiados
- Proceso de prestación de servicios
- Procesos de relaciones
- Procesos de resolución
- Procesos de control y liberación

Actualmente, se está realizando una revisión para alinear la norma con la ITIL v3, por lo que se está trabajando en dos partes más: una trata el modelo de procesos de referencia de gestión de servicios, que describe cómo se establecen las bases del modelo de madurez y el marco de evaluación; y la quinta y última requiere un ejemplar del plan de implementación para la norma; es la presentación de un ejemplar final de todas las tareas por realizar.

PARTES	DESCRIPCIÓN
I	Especificaciones
II	Código de buenas prácticas
III	Guía sobre la definición del alcance y aplicabilidad
IV	Modelo de procesos de referencia de gestión de servicios
V	Ejemplar del plan de implementación

***Tabla 2.** Partes de la versión 3 de ITIL.*

Luego de ver los detalles de la norma ISO20000, a continuación describiremos los pasos que se deben seguir en un proceso de certificación. Una vez que nuestra empresa haya implementado un sistema de gestión de servicios de IT (SGSIT), y haya decidido certificar, necesita realizar estas actividades. Habrá dos actores principales, que serán la empresa solicitante y la entidad certificadora. Estas tareas deben ser cubiertas por ambos para lograr la certificación:

- Determinar el alcance de la certificación dentro de la empresa. Acotar los límites en los cuales la norma tiene incidencia.
- Realizar una solicitud de la certificación ante la entidad certificadora. También es necesario analizar la documentación correspondiente a la norma y ver todos los requisitos que debe cumplir la empresa.
- Organizar una visita previa de la entidad certificadora a nuestra empresa, de esta forma será posible ultimar los detalles pendientes.
- Luego de que la entidad evalúe la situación, será necesario tomar una decisión considerando la devolución correspondiente.
- Si todo sale bien, recibir la concesión del certificado luego de que la empresa haya pasado satisfactoriamente la evaluación.



Figura 11. *Nos ponemos de acuerdo con la entidad certificadora para realizar la primera auditoría. El día indicado, realizamos la auditoría de la mejor manera posible.*

Podrían incluirse dos pasos más, que serían la auditoría de seguimiento anual y la renovación cada tres años, pero eso estaría fuera del proceso.

ANTIVIRUS CORPORATIVOS

Las máquinas de escritorio podrían ser las primeras en infectarse con un virus y podrían originar un ataque masivo a nuestra red. Entonces, los servidores y la continuidad del negocio sin duda se verían afectados. Los antivirus corporativos son una evolución de los comunes, usados fuera de una red empresarial. Tienen una configuración centralizada y varios módulos que detallaremos a continuación.

Características de los antivirus corporativos

Sin dudas, la evolución de los antivirus nació con el estudio de los de escritorio. Es por eso que los de servidores son mucho más potentes, tienen más opciones, más configuraciones, y abarcan la seguridad de la empresa como un todo. Además, centralizan información de toda la red y las descargas de actualizaciones, muy importante para unificar la seguridad. Incorporan todo un grupo de elementos, por ejemplo: antivirus, firewall, antispyware, antispam, analizadores de tráfico de red, etc. Las

empresas dedicadas al desarrollo de los antivirus de más renombre en este rubro, y que abarcan gran parte del mercado, son **Symantec** (**www.symantec.com/es**), **Trend Micro** (**http://es.trendmicro.com**) y **McAfee** (**www.mcafee.com/es**). Todas ellas ofrecen varias versiones de sus productos e infraestructuras, y dividen sus herramientas en usuarios domésticos (de 1 a 10 usuarios), empresas chicas (de 10 a 100 usuarios), medianas (de 100 a 1000) y grandes (más de 1000). Dependiendo del tamaño de la nuestra, elegiremos el que mejor se adapte a nuestro caso.



Figura 12. ***El sitio nos permite ver todas las opciones de productos y elegir el que mejor se adapte a nuestra empresa, según su tamaño.***

Estos antivirus nos aseguran tener una administración centralizada. Habrá un servidor central, que administre los clientes instalados en servidores y máquinas de escritorio. Los clientes, al querer actualizarse, buscarán las actualizaciones adecuadas en el servidor central de la empresa antes de hacerlo en Internet. Es posible dar acceso a Internet también, pero si sólo permitimos que se actualicen mediante nuestro servidor, nos aseguraremos de que todas las máquinas tengan las mismas versiones de defensa, y podremos analizar un problema o una intrusión con más facilidad. Los clientes reportarán todos sus detalles al servidor central, tendremos informes de posibles ataques, informes de programas instalados que puedan poner en riesgo el accionar de la compañía y de programas inseguros que deberán ser desinstalados. Si la seguridad de la empresa depende de nosotros, es fundamental estar muy

atentos ante cualquier ataque. Para hacerlo, es más que importante informarse a diario y suscribirse a los avisos de los principales sistemas antivirus y a **Microsoft Security Advisory** (**www.microsoft.com/technet/security/advisory**). Ante cualquier aparición de una vulnerabilidad, seremos conscientes de que si no realizamos las acciones necesarias para protegernos, podremos ser infectados o estafados. Otra característica importante de los antivirus corporativos es que podemos sacar de nuestra red las máquinas infectadas, ponerlas en cuarentena y bloquearles el acceso a la red. Así, podríamos detener un ataque fácilmente.



***Figura 13.** Smart Protection Network es el caballito de batalla de Trend. Se encuentra en el primer lugar de evaluación de malware en tiempo real.*

Infraestructura de los antivirus

Las soluciones de antivirus corporativos tienen varios servicios que debemos instalar. Es preciso proteger toda la infraestructura: servidores, máquinas de escritorio, accesos y egresos. Los servidores y las máquinas de escritorio tendrán instalados clientes, que reportarán a un servidor central, el cual será exclusivo de la aplicación de seguridad. Desde allí vamos a administrar y realizar reportes con la información que nos ofrecen los clientes, así como también con las otras aplicaciones de seguridad. Siempre nuestras instalaciones se dividirán en grandes o chicas, dependiendo del tamaño de la organización. A continuación, veremos algunos gráficos extraidos de los manuales de Symantec para instalar ambientes grandes y chicos. Esta solución de antivirus necesita, por lo menos, un servidor de Symantec y uno de base de datos para funcionar.

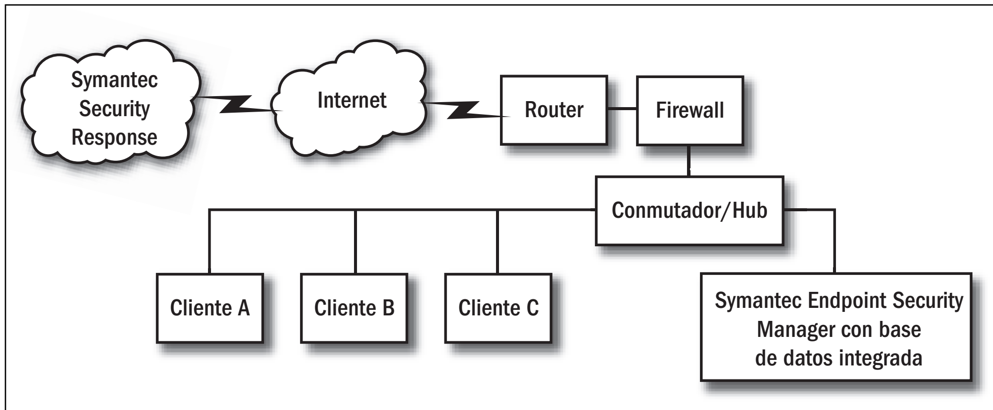


***Figura 14.** Este gráfico muestra cómo se vería nuestra infraestructura de antivirus en un ambiente chico, sin división de servicios, sin replicación.*

En el gráfico de la **Figura 14** vemos que el servidor de base de datos y el Symantec Endpoint Security Manager pueden instalarse en un único servidor para que cumpla los dos roles: controlador antivirus y almacenamiento de datos. El servidor es parte de nuestra red y está de frente a los clientes, sin ningún tipo de firewall en el medio. Si nuestra empresa es más grande, tendremos el gráfico de la **Figura 15**.

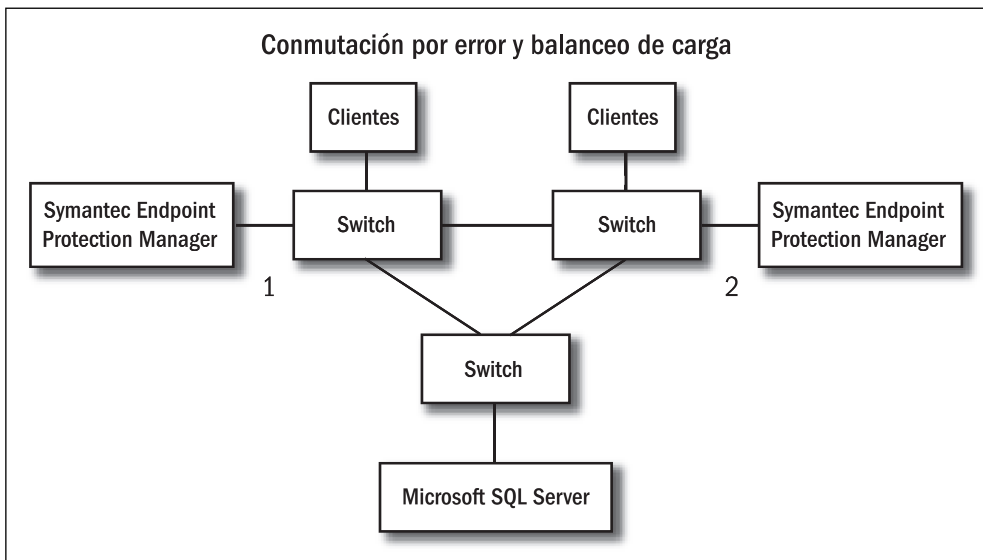


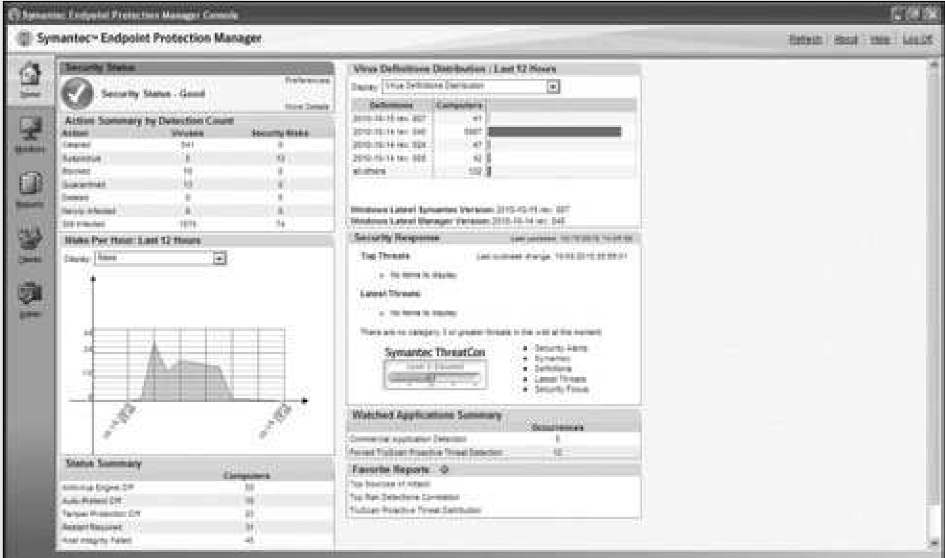
***Figura 15.** Si nuestra empresa es más grande, la instalación requerirá de dos o más servidores para controlar la gran cantidad de clientes en la red, y otro más para almacenar los datos.*

Al instalar Symantec en la forma que muestra la **Figura 15**, podremos tener balanceo de carga y control de errores, por si uno de los servidores falla.

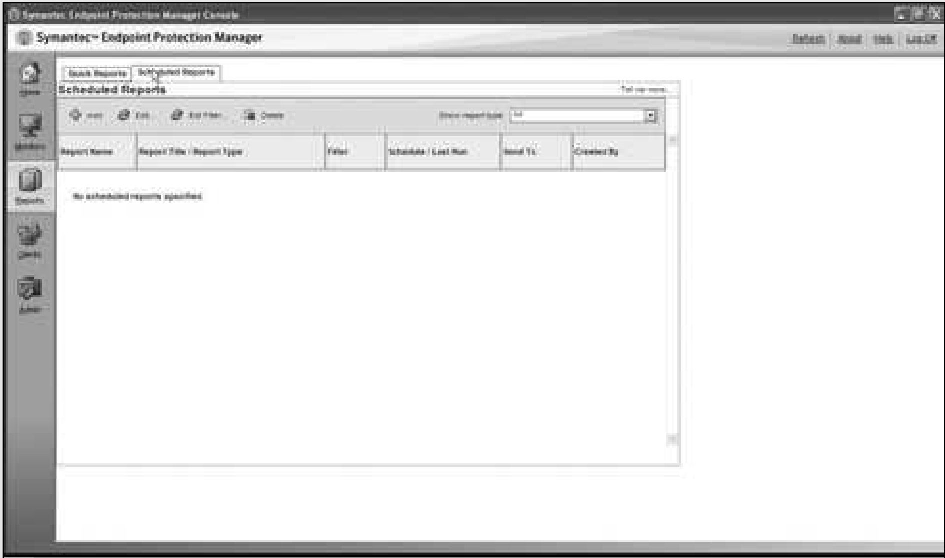
Crear un reporte programado con Symantec

PASO A PASO

1 En el servidor de Symantec Endpoint Security Manager diríjase a **Inicio/ Programas**, y abra la consola de administración de Symantec.



2 Para continuar, será necesario que oprima sobre el icono correspondiente a la opción denominada **Reports**, ubicado en la barra de herramientas del lado izquierdo, y elija la solapa **Scheduled Reports**.

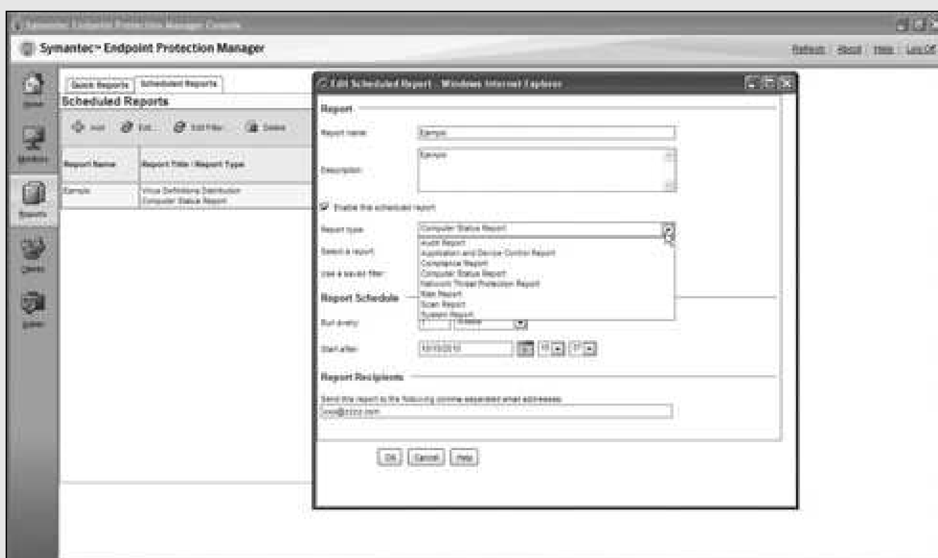


▶

3 Haga clic en **Add** para programar un nuevo reporte. Complete el nombre, una breve descripción, elija cada cuánto se va a repetir, e indique una fecha de inicio y un filtro en la lista desplegable **Use a saved filter**.



4 En este paso deberá seleccionar el tipo de reporte deseado en el menú desplegable llamado **Report Type**. En este caso, es **Computer Status Report**, para crear un reporte de estado de clientes.



▶

5 A continuación, cree un reporte de definición de actualización. Para hacerlo, del menú desplegable **Select a Report** seleccione el reporte de estado **Virus Definition Distribution**.



6 Por último, complete un e-mail y oprima **OK** para guardar el reporte creado.

FIREWALLS CORPORATIVOS

Según estadísticas del IDC (*International Data Corporation*), el FBI (*Federal Bureau of Investigation*), la CIA (*Central Intelligence Agency*) y de varios organismos más, el 98% de las empresas cuenta con algún sistema de firewall. Los firewalls son las puertas de entrada a nuestra empresa, por lo que debemos controlar el acceso de la manera adecuada, como controlamos el ingreso a nuestra casa. A continuación, conoceremos detalles de los firewalls lógicos y los físicos. Más adelante veremos cómo definir reglas de administración en ellos.

Firewalls físicos y lógicos

Estos sistemas están diseñados para bloquear el acceso no autorizado por ciertos canales de comunicación en nuestra red. Pueden limitar el tráfico y también cifrarlo, para ocultar datos hasta el destino. Otra función importante es que se los

puede utilizar como gateways (puertas de enlace) entre distintas redes. Los gateways interconectan redes con protocolos y arquitecturas diferentes. Traducen la información utilizada en un protocolo de red al usado en otra. Los protocolos emplean puertos que habilitaremos y deshabilitaremos dependiendo de lo que permitamos que se haga en la red. Cada aplicación utiliza determinados protocolos. Por ejemplo, Internet usa el HTTP y los puertos 80 y 8080, las aplicaciones de FTP utilizan el puerto 21, el servicio de correo electrónico que trabaja con el protocolo POP3 usa el puerto 110, etc.

Veamos un ejemplo que nos permitirá entender mejor todos estos conceptos. Hagamos una analogía entre la comunicación entre dos máquinas y una terminal de ómnibus. En la terminal (computadora) vemos 65.535 andenes numerados (puertos de la computadora), cada uno perteneciente a una empresa distinta de viajes (protocolo de comunicación). Si nosotros (en la analogía seríamos un dato que quiere viajar de una máquina a otra) utilizamos para viajar una empresa X (Internet, por ejemplo), sabemos que ésta tiene el andén 80, que es el que debemos utilizar. Nuestros destinos serán otras terminales de ómnibus (otras máquinas). Entonces, nuestro viaje saldrá por el andén 80 y llegará a la otra estación, también al andén 80. Allí esperamos a ser transportados (ésos son los puertos que el administrador debe dejar abiertos para esa aplicación). Ahora, si uno de los ómnibus de la empresa X quiere entrar por el andén 4593, el oficial de seguridad de la terminal (firewall) no se lo permitirá (este puerto estará deshabilitado para ese protocolo), porque lo utilizará otra empresa o no tendrá uso. El firewall es ese oficial de nuestra terminal de ejemplo. Sin la seguridad del firewall, el tráfico sería un caos, y cualquier paquete de información podría llegar a cualquier puerto de nuestro servidor y, así, entrar sin permiso a la red.

Este tipo de firewalls son físicos (hardware). Pueden bloquear conexiones por puertos o direcciones de IP o MAC, pero no, una máquina que cambia de dirección IP constantemente. Entonces, si dentro de un protocolo HTTP queremos bloquear todas las conexiones a los sitios que contengan la palabra **virus**, los firewalls físicos podrán bloquear sólo direcciones de IP, por lo que tendremos que cargar continuamente direcciones por ser bloqueadas según una búsqueda previa. Es allí donde nos encontramos con los firewalls lógicos, que trabajan a nivel de aplicación, dentro de



GENERACIONES DE FIREWALLS

Debemos saber que los firewalls físicos son considerados de primera generación, y los lógicos, de segunda generación. Los primeros son más especializados en el filtrado de paquetes, pero los segundos también pueden realizar esta tarea en forma correcta. En la actualidad, las empresas utilizan ambas soluciones en forma combinada.

cada protocolo. Entonces, para bloquear estos sitios, precisamos configurar una regla que nos diga que se cierren todas las conexiones en donde el nombre del sitio por conectar contenga la palabra **virus**. Tengamos en cuenta que, hoy en día, también los firewalls físicos pueden cumplir funciones avanzadas y actuar como lógicos. Un gran ejemplo de firewall lógico es el **ISA Server** (*Internet Security and Acceleration Server*), de Microsoft. Actualmente, pertenece a la solución integral de seguridad de Microsoft llamada **Forefront**, por lo que el producto cambió de nombre y se conoce como **Forefront TMG**. Éste, como tantos otros firewalls lógicos, es utilizado como **proxy** para la red de la empresa. Los proxys son programas o dispositivos que realizan una acción en nombre de otro. Son intermediarios de comunicación, y es ahí donde actúa el firewall. Los dispositivos de nuestra red no se conectan directamente a Internet, sino que lo hacen a través del proxy. Éste, a su vez, estará conectado a un firewall físico para blindar el acceso a la empresa. No sólo da control a la red, sino que también brinda velocidad, ya que funciona con una memoria caché para el tráfico.

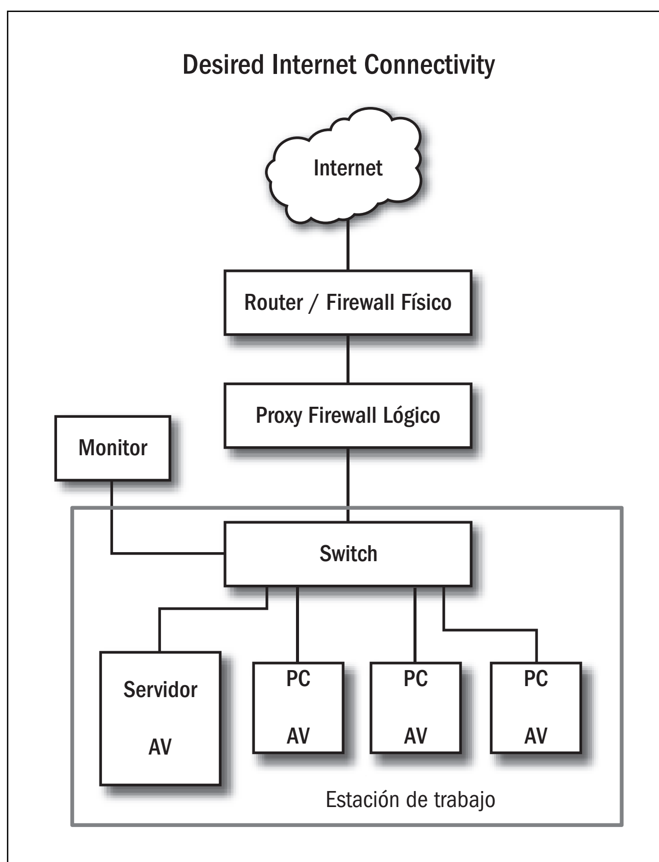


***Figura 16.** Éste es el esquema que debemos tener en nuestra empresa: un firewall físico de cara a Internet y otro lógico detrás.*

Definición de reglas de seguridad

La definición de reglas en los firewalls no es nada más y nada menos que establecer un bloqueo o una habilitación de cierto protocolo y puerto. Por ejemplo, podremos bloquear el protocolo HTTP para todos los puertos menos el 80 y el 8080. ¿Pero bloqueamos todos los puertos o sólo habilitamos esos dos para que exista comunicación? Hay dos políticas básicas y formas de realizar las configuraciones que tienen que ver con la filosofía de la seguridad dentro de la empresa:

- **Política restrictiva**
- **Política permisiva**

Adoptando la primera, debemos denegar todo el tráfico excepto el que esté explícitamente permitido. Entonces, cerramos todos los puertos de comunicación, y habilitamos los protocolos y los puertos que utilicemos.
La segunda es un poco más blanda, ya que con ella permitimos todo el tráfico excepto el que esté explícitamente denegado; es decir que dejamos todos los puertos abiertos y bloqueamos sólo aquellos que nos parezcan una amenaza. Tanto los firewalls físicos como los lógicos tienen una interfaz para configurarlos. Los físicos poseen un minisistema operativo que publica una página web a la cual podemos acceder mediante su dirección IP, y allí configurarlos. Antes sólo se los podía configurar mediante una conexión Telnet o con un cable serial. Los lógicos cuentan con sus propias consolas o disponen de un acceso web.

... RESUMEN

Al principio del capítulo conocimos qué son las políticas y cómo configurarlas, y también vimos qué nos traen de nuevo las últimas plataformas de Microsoft. Luego, vimos detalles sobre los centros de cómputos y entendimos cómo se vería afectada la continuidad del negocio si se produjera algún desastre. Por eso, aprendimos a estar preparados haciendo un plan de contingencias acorde. Conocimos también qué son las normas dentro de nuestra administración, cuáles son las más importantes y, para finalizar, detallamos la seguridad a nivel antivirus corporativo y aplicación de firewalls.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 ¿Qué es una política de seguridad y con qué herramienta se administra?

2 ¿Qué características nuevas incorporan Windows 2008 y Windows 7 con respecto a las políticas?

3 Describa los elementos que pueden encontrarse en los centros de cómputos.

4 ¿Cómo se realiza un chequeo diario?

5 ¿Qué contingencias podrían ocurrir en los centros de cómputos?

6 ¿Qué son las normas ISO?

7 ¿Qué ofrecen las normas ISO9001 y 27001?

8 ¿Qué son las normas ITIL y cómo se relacionan con la norma ISO20000?

9 ¿Cuáles son los principales proveedores del mercado de antivirus?

10 Describa los distintos tipos de firewalls que existen.

EJERCICIOS PRÁCTICOS

1 Realice un plan de contingencias propio e impleméntelo.

2 Analice qué políticas lo ayudarían a realizar una mejor administración.

3 Detalle las características de los nueve libros de ITIL.

4 Verifique la instalación de firewalls en su empresa.

5 Investigue las ventajas y desventajas de tener una política restrictiva o permisiva en los firewalls.

Virtualización de servidores

Para poner en marcha un nuevo servicio, pedimos el presupuesto de un nuevo servidor, lo rackeamos, lo cableamos, lo encendemos y comenzamos a configurar el array de discos. Luego instalamos el sistema operativo y la aplicación, comenzamos con las pruebas en preproducción y ponemos en marcha la aplicación. Esto demanda entre tres y cuatro semanas. Por medio de la virtualización lo realizaremos en solo cinco minutos.

DEFINICIÓN DE VIRTUALIZACIÓN

Hemos escuchado mucho la palabra virtualización en estos últimos años. Seguramente, tendremos algún colega que esté empezando a preocuparse por no entender este concepto, con miedo de quedarse atrás en cuanto a los avances de la tecnología. Otro concepto que viene de la mano de éste es el de computación en la nube, con lo cual ya se van sumando más. La tecnología está comenzando a crecer, como lo hizo el hardware hace unos años, de manera exponencial. En esta primera parte del capítulo, definiremos estos conceptos, y veremos qué empresas se encuentran en este mercado, junto con sus más recientes productos.

Qué es la virtualización

Durante varios años, el crecimiento tecnológico del hardware fue más rápido que el del software. El hardware se expandía en capacidad y velocidad de procesamiento, pero no había software que tomara ese crecimiento y lo explotara al máximo. Imaginemos el servidor de una aplicación que contenga tan sólo los datos de facturación. El uso que puede llegar a tener durante el mes es muy poco: sólo deberemos actualizar los datos con cierta frecuencia y, tal vez, efectuar alguna que otra consulta. El uso de la CPU, en promedio, en esos días será del 10% del total como mucho. Por el contrario, a fin de mes, cuando llega el momento de presentar todos los informes y hacer un cierre de la facturación, el uso será casi del 100% o, en ciertas ocasiones, del 130%. En resumen, el hardware estará desaprovechado; sin embargo, hasta ahora no había forma de ahorrar en la compra de los equipos. Indefectiblemente, el hardware era necesario a fin de mes, aunque durante el resto de los días no se aprovechara su poder de cálculo. La virtualización de servidores viene a darnos una solución para este inconveniente: nos brinda ahorro, agilidad en la administración y aprovechamiento del hardware al máximo.
La virtualización nos permite usar toda la capacidad de nuestros servidores durante el mayor tiempo posible. Así, podemos exprimir nuestros recursos de hardware sin gastar de más. Nos da la posibilidad de tener varios servidores en uno solo y, de este modo, compartir todos los recursos. Por ejemplo, podemos virtualizar nuestro



VIRTUALIZACIÓN

Seguramente, a lo largo de nuestros años de estudios, habremos escuchado más de una definición sobre esta tecnología, pero para simplificarla podemos decir que es una técnica avanzada para compartir los recursos de hardware de la mejor forma posible, ahorrando dinero, y maximizando los recursos económicos y administrativos que giran en torno al manejo de servidores.

sistema de base de datos y compartir el hardware con algún otro servidor, como uno de archivos o de impresión. La virtualización pone una capa de tecnología entre el hardware y el sistema operativo; hace creer a este último que está instalado en un equipo físico cuando, en realidad, está virtualizado. Un servidor virtualizado se comportará de la misma forma o mejor que uno físico.

***Figura 1.** Un único servidor físico puede albergar varios servidores virtuales para aprovechar los recursos de memoria, CPU y almacenamiento.*

Veremos más adelante que podemos transportarlos fácilmente entre distintos servidores físicos, lo que significa una gran agilidad a la hora de recomponer un sistema físico en mal estado. El servidor de virtualización fabrica hardware virtual para que el sistema operativo crea que es un servidor físico. El hardware virtual es independiente de cualquier plataforma y siempre utiliza los mismos drivers. Es por eso que, cualquiera sea el lugar a donde lo movamos, siempre podremos ponerlo en marcha sin inconvenientes. Lo que sí debemos tener en cuenta es usar siempre la misma plataforma de virtualización, ya que hay muchas en el mercado y, realmente, no son compatibles unas con otras. Más adelante veremos que esta práctica puede automatizarse y, así, tener el ambiente de servidores sin pérdida alguna de datos. Sin dudas, las empresas están poniendo foco en la virtualización y esto se ve reflejado en el informe de la prestigiosa consultora **Gartner**.



GARTNER

Debemos saber que se trata de un proyecto de investigación de tecnologías IT, cuya sede principal se encuentra en Stanford, Estados Unidos. Esta agencia de informes es la más prestigiosa en el ambiente de IT y una de las que más atención se lleva de los CEOs. Fue fundada durante el año 1979 y trabajan en ella empleados de 75 naciones.



Las Estrategías tecnológicas de los CIOs reflejan un aumento de interés por soluciones de peso más livianas.

Tecnologías CIO	Ranking de tecnologías seleccionadas por los CIOs dentro del top 5 de prioridades para el año 2010				
Ranking	2010		2009	2008	2007
Virtualización	1	↑	3	3	5
Cloud Computing	2	↑	16	*	*
Web 2.0	3	↑	15	15	*
Redes, comunicaciones de voz y datos	4	↑	6	7	4
Business Intelligence (BI)	5	↓	1	1	1
Tecnologías móviles	6	↑	12	12	11
Administración y almacenamiento de datos	7	↑	10	9	9
Servicios orientados a aplicaciones y arquitectura	8	↑	9	10	7
Tecnología de seguridad	9	↓	8	5	6
Administración IT	10		*	*	*
Aplicaciones empresariales	11	↓	2	2	2

* Nueva pregunta para el año

***Figura 2.** El informe coloca a la virtualización en el primer puesto, cuando en años anteriores estaba en el tercero. Sin dudas, es la base para el cloud computing, ubicado en el segundo lugar, que subió 15 posiciones en el ranking.*

A continuación, veremos algunas empresas del rubro y las soluciones que ofrecen para el mercado actual. El crecimiento imparable de la virtualización hace que cada vez haya más competencia y más investigación sobre esta tecnología.

Empresas en el mercado y sus soluciones

El concepto de virtualización comenzó en los laboratorios de la empresa IBM en la década del 60. Científicos de la prestigiosa compañía pensaron en dividir la gran capacidad de cómputo de los robustos mainframes para así aprovecharlos al máximo. Ellos notaron que una gran capacidad de cómputo se perdía en forma irremediable, al mantener ocioso el sistema. El primer mainframe fabricado por IBM para dar soporte a la virtualización fue el IBM S/360 modelo 67, que comenzó a producirse el 7 de abril del año 1964. Estos equipos quebraron varios récords y son reconocidos en la historia de la informática por varios sucesos importantes. Por ejemplo, fueron las primeras computadoras atacadas por un virus informático, el denominado **Creeper**, que mostraba en pantalla la leyenda en inglés: **I'm a creeper. Catch me if you can!** (algo así como "soy una enredadera, agárrame si puedes"). Otro motivo por el que son reconocidos es que fueron los primeros equipos en permitir acceso remoto mediante una conexión telefónica.
Es interesante saber que el modelo 67 fue anunciado en agosto del año 1965 y traía consigo el sistema operativo conocido como CP/CMS, el primer sistema de máquina virtual de la historia. Se fabricó en el Centro Científico de Cambridge en cooperación con los investigadores del MIT (*Massachusetts Institute of Technology*). Luego le siguieron el modelo S/370, pero más tarde, en las décadas del 80 y el 90, el mercado y las empresas abandonaron un poco la idea.

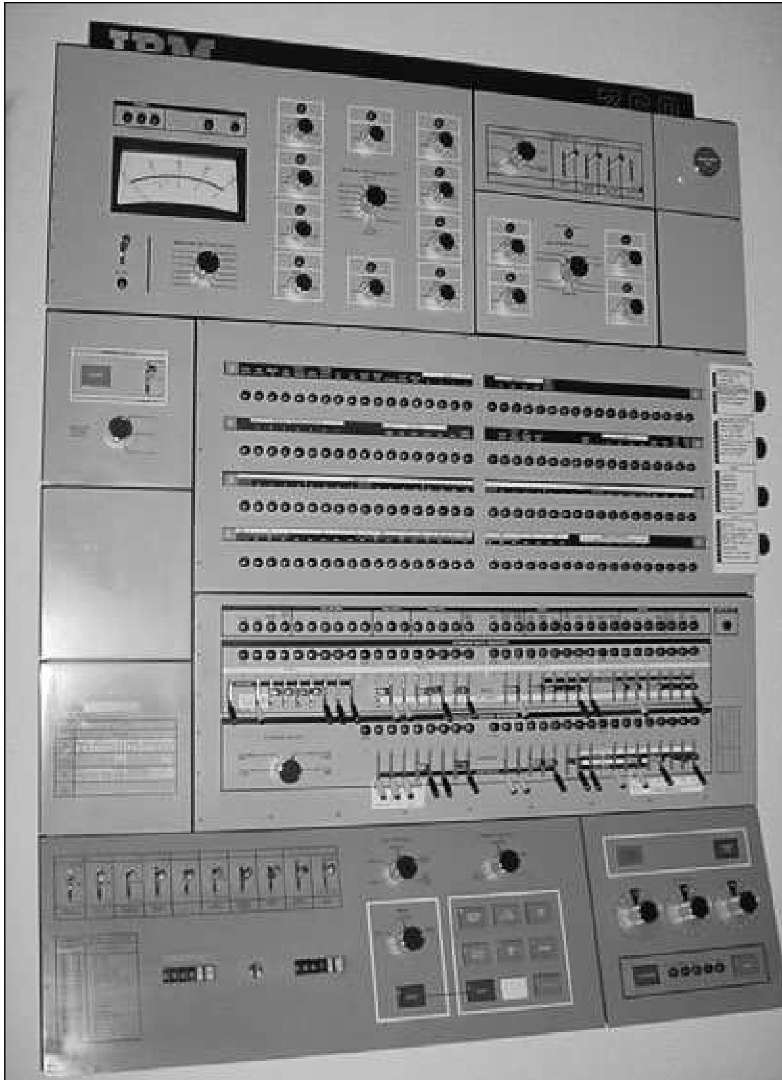


***Figura 3.** Así se veía el panel de control del mainframe S/360. Todos los paneles de los distintos modelos eran parecidos, muy distintos de lo que estamos acostumbrados a ver hoy en día. La virtualización no es algo nuevo.*

Con el advenimiento de las nuevas plataformas x86, de gran cantidad de servidores y de switches, surgió la necesidad de virtualizar en ellas, porque se generaban grandes problemas de infraestructura y administración. VMware fue la empresa que desarrolló la virtualización sobre esta plataforma, y hoy es líder en el mercado. En la actualidad, es muy raro ver equipos mainframe por los altos gastos que generan; sólo se usan en trabajos muy específicos. VMware le lleva una ventaja de diez años de especialización a soluciones posteriores, como la de Microsoft. Más adelante veremos las empresas que hoy en día son reconocidas por los grandes analistas.

Desafíos

Líderes

VMware

Microsoft

Capacidad de ejecución

Oracle VM

Red Hat

CTRIX

Oracle Solaris Containers

Red Parallels

Novell

Nichos de negocios

Visionarios

Integridad de visión

***Figura 4.** En el cuadro vemos las cuatro ubicaciones de las empresas de virtualización que se presentaron en el informe de Gartner para 2010. Actualmente, Microsoft se alió con Citrix para darle batalla a VMware.*

Según la famosa consultora Gartner, VMware es el líder en virtualización; Microsoft es su gran competidor; Citrix es considerado como visionario en la industria; y



DRS

Es interesante saber que DRS viene del inglés **Distributed Resource Scheluder**, y permite que nuestro Virtual Center se convierta en una granja de carga balanceada. Si un nodo está sobreexigido, el DRS lo mueve automáticamente hacia otro nodo. Existen varios grados de este sistema, que pueden ser más agresivos o tan sólo informativos.

Oracle VM, Oracle Solaris Containers, RedHat, Parallels y Novel son pequeños jugadores o nuevos nichos de negocio. Como Citrix y Microsoft están aliadas en la actualidad, este cuadro seguramente cambiará mucho para 2011 (quizá no se las separare como competidoras). Las soluciones ofrecidas son las siguientes:

EMPRESA	SOLUCIÓN	WEB
VMware	Vsphere	**www.vmware.com/products/vsphere**
Microsoft	Hyper-V	**www.microsoft.com/hyper-v-server**
Citrix	XenServer	**www.citrix.com/xenserver**
Oracle	Oracle VM	**www.oracle.com/us/technologies/virtualization**
Oracle Solaris	Oracle Solaris Containers	**www.oracle.com/us/products/servers-storage/solaris/virtualization**
Red Hat	Enterprise Virtualization	**www.latam.redhat.com/rhel/virtualization**
Parallels	Parallels Server	**www.parallels.com/virtualization/server**
Novell	Suse Linux Enterprise Server	**www.novell.com/es-es/products/server/virtualization.html**

Tabla 1. *Principales vendedores de soluciones de virtualización.*

Todas las empresas aquí nombradas ofrecen variadas soluciones de virtualización. Podemos encontrar ofertas para servidores, para máquinas de escritorio, para almacenamiento de datos, etc. VMware es la pionera y lidera el mercado, y es por eso que en este libro nos centraremos en su producto.

VMWARE

Esta firma ofrece una robusta solución para empresas, aunque también para medianos y pequeños usuarios. Permite fácilmente virtualizar equipos y administrarlos de forma ágil, a la vez que monitorizar cualquier cambio que haya en ellos. Nos centraremos, en este caso, en la solución para servidores. A continuación, veremos la infraestructura que necesitamos instalar, conoceremos cómo se tratan las licencias, daremos unos ejemplos de instalación y aprenderemos a crear máquinas virtuales. Más adelante, nos referiremos al networking y a las actividades que pueden realizarse en las consolas gráficas y de línea de comando.

Infraestructura de la solución de VMware

La empresa VMware cuenta con gran diversidad de soluciones de virtualización, pero, como ya mencionamos, nosotros nos centraremos en la dedicada a servidores. Veremos los productos iniciales y, más adelante, en el **Capítulo 5**, conoceremos los empresariales, que nos permitirán escalar nuestra infraestructura de manera inimaginable. La solución de VMware está compuesta por varios productos.

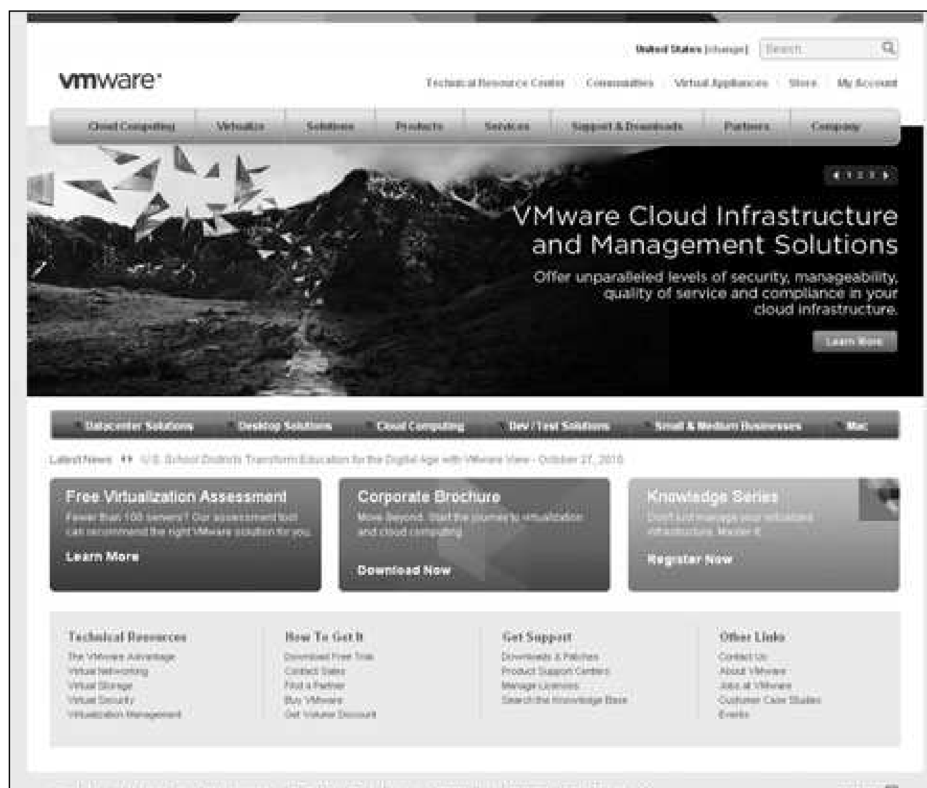


***Figura 5.** Hay varias opciones de herramientas en el sitio de VMware (**URL www.vmware.com**) para investigar y probar.*

Primero y principal, tenemos **VMware Server**, **VMware Workstation** y **VMware Player**. Workstation y Player son usadas en ambientes pequeños y de testing. En este último tiempo, la firma ha cambiado un poco la situación de estas herramientas, al hacer que casi no haya distinción entre ellas, pero las hay. Player antes se utilizaba para correr una sola máquina virtual y nada más. Servía para utilizar otro sistema operativo, pero no podíamos crear una máquina virtual desde cero ni modificarla. En la versión 3.1, la última disponible al momento de la redacción de este libro, podemos crear máquinas virtuales, modificarlas, utilizarlas al



VMWARE PLAYER EN VEZ DE XP MODE

Gran cantidad de usuarios recomiendan el uso de VMware Player en Windows 7 en reemplazo de Windows XP Mode. Este último consume muchos más recursos, en tanto que VMware Player administra con más eficiencia el acceso a la CPU y la memoria de la computadora, ofreciéndonos una mejor experiencia de acceso a un sistema operativo Windows XP.

mismo tiempo si abrimos varias instancias, y más, siempre con licencias gratuitas. La versión Workstation es un poco más avanzada y alrededor de octubre de 2010 VMware liberó su licencia, por lo que podemos utilizarla de forma gratuita. Hace un mejor uso y administración del hardware y trae más funcionalidades; por ejemplo, podemos utilizar snapshots para tomar una imagen congelada del estado de nuestras máquinas virtuales. También, podemos realizar alguna aplicación para el ambiente virtual, ya que se integra con Visual Studio, Eclipse y otros entornos de desarrollo. Para la enseñanza y la realización de cursos, también es muy importante, porque permite armar un ambiente de servidores virtuales para estudiantes con el fin de utilizarlo en algún curso y, luego, volver todo a un estado anterior. Si bien esta versión cuenta con varias características más avanzadas que la Player, en ambas, si se cierran, se cierran todas las máquinas virtuales. Ésta es una característica que distingue al VMware Server, ya que actúa como un servicio; es la antesala a la versión ESX.
VMware Server es la solución definitiva para la virtualización bajo un sistema operativo Windows o Linux. Se instala fácilmente (hasta en cualquier servidor x86) y es posible acceder en forma remota desde cualquier máquina utilizando **VMware Remote Console**. Podremos bajar máquinas virtuales directamente desde Internet, es más escalable, se pueden manipular máquinas virtuales de hasta 8 GB de memoria RAM y manejar más de 10 tarjetas virtuales de red para cada equipo; también soporta dispositivos USB 2.0 virtuales y dispositivos SCSI. Sin dudas, es la mejor elección de las tres, sobre todo, por ser gratuita en la actualidad. Otra razón es que, en comparación con otras versiones que veremos más adelante, las ESX y ESXi, VMware Server no necesita un hardware dedicado, sino que se puede compartir con otros servicios si estamos escasos de recursos.
Las versiones **ESX** y **ESXi** están un poco más orientadas a las aplicaciones empresariales, que tienen más demanda. Ofrecen más resguardo para aplicaciones críticas y son el comienzo para escalar a la mejor opción de virtualización: **VMware vSphere** (veremos su explicación detallada en el **Capítulo 5**). Los servidores ESX y ESXi traen un sistema operativo creado por VMware para uso exclusivo de virtualización. Son sistemas basados en Linux, adaptados y personalizados por investigadores y grupos de desarrolladores de VMware. Las licencias que utiliza ESXi son gratuitas, a diferencia de las correspondientes a la ESX. La diferencia principal entre estos dos productos está



COMPATIBILIDAD CON VMWARE

En el sitio **www.vmware.com/resources/compatibility/search.php**, se puede chequear la compatibilidad de los productos VMware con el hardware y sistemas operativos que serán instalados en máquinas virtuales. Tan sólo debemos elegir una forma de búsqueda de varias combinaciones posibles, y el sitio arrojará los resultados con la documentación correspondiente.

en su arquitectura y su administración. El sistema operativo de la versión ESX se compone del **vmkernel** (core Linux adaptado VMware) y el **COS** (*Console Operating System*, o consola de sistema operativo); en cambio, en ESXi la consola de servicio fue extraída, lo cual le da más seguridad porque concentra la administración por consola en otro servidor, como lo requieren ciertos estándares. Ya no se puede acceder por web y todos los errores que COS podría llegar a traer fueron eliminados, junto a sus 2 GB de información. La actualización de ESXi es mucho más rápida de esta manera. La empresa ha cambiado el nombre de ESXi por **VMware vSphere Hypervisor**, preparándose para dejar atrás la versión de ESX paga. La razón principal es que ESXi es más liviana y segura. En un primer momento, la versión ESX fue muy importante, pero ESXi se volvió fuerte en el rubro de seguridad. Estos sistemas sólo funcionan en servidores con capacidad de virtualización a nivel microprocesador.

Tanto ESX como ESXi se habilitan para ser contactados por un cliente de conexión **VMware vSphere Client**, una aplicación de escritorio que interactúa con el servidor conectándose de forma remota. En cada servidor ESX/ESXi podemos crear varias máquinas virtuales; la cantidad depende de los recursos físicos del servidor, principalmente, de la cantidad de memoria RAM, el espacio en disco y la capacidad del microprocesador. Seguramente, vamos a instalar más de un servidor ESX o ESXi, cada uno con distintos recursos para compartir y diferentes servidores virtuales. Todos pueden administrarse en conjunto si instalamos **VMware Virtual Center** o **VMware Vsphere**. Ambos sistemas necesitan una base de datos y deben ser instalados sobre un servidor de plataforma Windows. Más adelante veremos los detalles de VMware Virtual Center, también llamado vCenter, y el próximo capítulo lo dedicaremos a VMware vSphere.

Hasta ahora, vimos que tenemos VMware Player, VMware Workstation y VMware Server, los servidores ESX y ESXi con sistema operativo propio vmkernel, VMware vSphere Client para administración remota, Virtual Center y Vsphere. Existen otras herramientas que conforman la infraestructura de la solución, y una de las más importantes es VMware vCenter Converter. Con ella podremos migrar máquinas virtuales entre plataformas y virtualizar servidores físicos. Es, sin dudas, un arma letal contra la competencia y se ofrece en forma gratuita. Otras opciones que podemos nombrar son **VMware vCenter Tool**, **vCenter Upgrade**, **VMware vCenter**



INSTALAR VMWARE TOOLS

Si no lo hacemos, no podremos utilizar todas las características y capacidades que nos ofrece VMware. El mouse se moverá lentamente y de una forma extraña al querer acceder al equipo. Si instalamos las herramientas, no distinguiremos si estamos en el servidor virtual o en nuestro escritorio. La velocidad de intercambio aumenta notablemente.

Orchestrator, **VMware Fusion** y **VMware Lab Manager**. vCenter Tool es un grupo de características que se instalan en las máquinas virtuales, y están compuestas por hardware virtual, drivers y conectores contra el servidor que la contiene.



***Figura 6.** VMware tiene contacto con todos los sistemas operativos del mercado, entre ellos, Windows, Mac OSX y Linux.*

Con vCenter Upgrade podremos actualizar nuestro servidor vSphere, los servidores ESX/ESXi y las VMware Tools en cada máquina virtual. VMware Orchestrator se utiliza para automatizar tareas que realizamos en forma manual. Hay distintas opciones para elegir que pueden sernos de gran ayuda para acortar tiempos. VMware Fusion, en su actual versión 3, permite hacer funcionar máquinas virtuales en plataformas Mac, de Apple. La última novedad es que podemos tener Windows 7 corriendo dentro de una Mac. VMware Lab Manager se utiliza para fabricar laboratorios de forma rápida, aprovechando la capacidad de clonación de equipos. A continuación, veremos un resumen de todas las herramientas nombradas.



LUN

Es una unidad lógica creada en los storage para administrar los discos. Se conecta mediante fibra a los servidores. Un mismo storage tiene varias LUNs. Cada una se conforma de varios discos y hasta pueden compartir discos entre ellas. Una LUN tiene un número unívoco que se debe configurar en las placas de fibra conectadas al servidor para que las distinga en el storage.

HERRAMIENTAS	DESCRIPCIÓN
VMware Player	Se utiliza para crear máquinas virtuales en testing. Corren en forma individual. Gratuita.
VMware Workstation	Permite crear varias máquinas virtuales en el escritorio, obtener snapshots y clonar equipos. La licencia es paga.
VMware Server	Permite correr y administrar varias máquinas virtuales al mismo tiempo con mayor grado de seguridad a nivel servicio. Antesala de la versión ESX. Ahora también es gratuita.
ESX	Es un servidor con sistema operativo Linux adaptado por VMware, que funciona como Hypervisor de máquinas virtuales. La licencia es paga. Se licencia por core de CPU.
ESXi o VMware vSphere Hypervisor	Es similar a ESX, pero su licencia es gratuita. Tiene menos características de configuración y sólo trae el kernel de VMware. En poco tiempo será el reemplazo de la versión ESX anunciada por la empresa.
VMware vSphere Client	Se utiliza como cliente de escritorio para contactarse contra el servidor ESX. Viene incluida en las versiones de ESX, ESXi, Virtual center y vSphere.
Virtual Center	Administra varios servidores ESX que se pueden agrupar en clusters y agrega funcionalidades como actualizaciones centradas. Funciona como servidor de licencias, agrega la característica de poder mover una máquina virtual de un servidor a otro, y más. Necesita de una licencia paga.
vSphere	Es una versión avanzada de Virtual Center. Puede manejar distintos clusters de servidores, agrega la capacidad de mover máquinas no sólo de servidor físico, sino también de ubicación en el storage. Agrega características que veremos más adelante, como HA, DRS, Fault Tolerance, etc. Tiene licencia.
Converter	Se utiliza para convertir máquinas físicas a virtuales.
VMware Tool	Debe instalarse en cada máquina virtual para acceder a todas las características y capacidades.
Orchestrator	Se utiliza para automatizar tareas administrativas.
Fusion	Es utilizada en máquinas Mac para virtualización de equipos. No es gratuita.

Tabla 2. *Productos destacados de VMware.*

Debemos tener en cuenta que el listado presentado en la tabla anterior no reúne todas las alternativas, ya que existen otras herramientas adicionales, que iremos nombrando más adelante a medida que tengamos más conocimientos sobre las utilidades básicas. Otros productos de VMware se detallan en la **Figura 7**.

CLON Y TEMPLATE

Los clones son tan sólo copias de servidores, mientras que los templates nacen de crear un clon. El clon queda agregado directamente a la consola como un nuevo servidor; el template queda guardado y apagado para que se creen copias a partir de él. Un template puede convertirse en un server y, así, destruirse como template en caso de que no lo necesitemos más.

Índice de productos

CENTRO DE DATOS E INFRAESTRUCTURA EN CLOUD
VMware vSphere
VMware vCloud Director
Familia de productos VMware vCenter
VMware Server
VMware vSphere Hypervisor (ESXi)

PRODUCTOS DE SEGURIDAD
Familia de productos VMware vShield
VMware vShield App
VMware vShield Edge
VMware vShield Endpoint

OTROS
VMware Data Recovery
VMware VMmark
VMware Capacity Planner
Cisco Nexus 1000V
VMware Compliance Checker
SUSE Linux Enterprise Server for VMware

INFORMÁTICA PARA EL USUARIO FINAL Y EL ESCRITORIO
VMware View
VMware ThinApp
VMware ACE
VMware Workstation
VMware Player
Zimbra
VMware Mobile Virtualization Platform (MVP)

PRODUCTOS DE MAC
VMware Fusion

PLATAFORMA DE APLICACIONES
VMware vFabric tc Server
VMware vFabric Hyperic

GESTIÓN DE ACTIVIDAD DE TI
VMware vCenter Chargeback
VMware Service Manager

GESTIÓN DE OPERACIONES E INFRAESTRUCTURA
VMware vCenter Server
VMware vCenter Server Heartbeat
VMware vCenter Orchestrator
VMware vCenter Site Recovery Manager
VMware vCenter Lab Manager
VMware vCenter Capacity IQ
VMware vCenter Configuration Manager
VMware vCenter Converter

GESTIÓN DE APLICACIONES
VMware vCenter Application Discovery Manager
VMware vCenter AppSpeed
VMware Studio

Figura 7. *El listado de productos que nos ofrece VMware es muy amplio y se encuentra dividido en categorías para que podamos encontrar la herramienta deseada en forma fácil.*

Cómo instalar ESX y ESXi

Ya explicamos la principal diferencia entre estos dos sistemas; veremos a continuación cómo se realiza la instalación de ambos. Los dos son muy similares, por lo que no haremos distinción entre uno y otro: cuando nos refiramos a ESX, estaremos incluyendo también a ESXi. Como primer paso, deberemos bajar el .ISO y quemarlo en un DVD o CD, dependiendo de la versión. Es muy sencillo de instalar. Sólo colocamos el sistema operativo en la unidad de CD o DVD y seguimos los pasos que se detallan a continuación. Vamos a mostrar la instalación conectados al servidor desde una consola física remota al centro de cómputos. También podemos instalarlo conectados directamente al equipo.



SERVIDOR DE LICENCIAS VCENTER/VSPHERE

Si por alguna razón los equipos que funcionan como servidores de licencias fallan, dejarán sin licencias a los que apuntan la licencia hacia ellos. Si se llega a romper el servidor, tenemos alrededor de 40 días para ponerlo en línea nuevamente. Luego de ese tiempo, nuestros ESX se quedarán sin licencia y volverán al estado de prueba por un período determinado.

Cómo instalar un servidor ESX/ESXi — PASO A PASO

1 Ponga en funcionamiento el servidor con el CD o DVD en la unidad lectora. Todos los datos del disco rígido se borrarán. Oprima **Next**.



2 Luego presione **Yes** para cargar los controladores al equipo.



▶

3 Una vez cargados los drivers, ingrese los datos de las licencias, si los tiene, o elija la opción **Enter a serial number later**. Oprima **Next**.

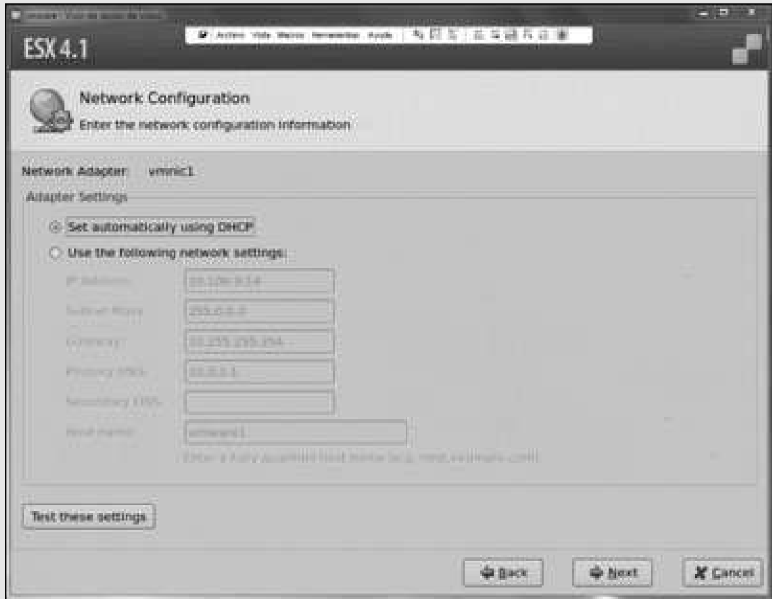


4 Elija la placa de red con la que trabajará. Figurarán en verde las que estén con un cable conectadas. Escoja la correcta y oprima el botón **Next**.



▶

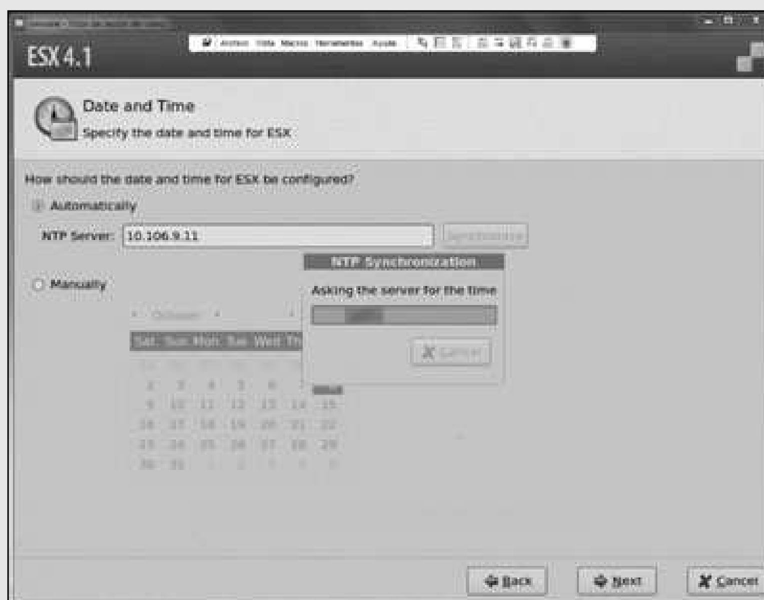
5 Ingrese la configuración de red. Luego, presione **Test these settings** para que la configuración de red tenga efecto. Oprima **OK** y, luego, en **Next**.



6 Elija la forma en que particionará los discos. Así se dividirá el disco para el funcionamiento de ESX. Oprima **Next**. Luego acepte y presione **Next**.



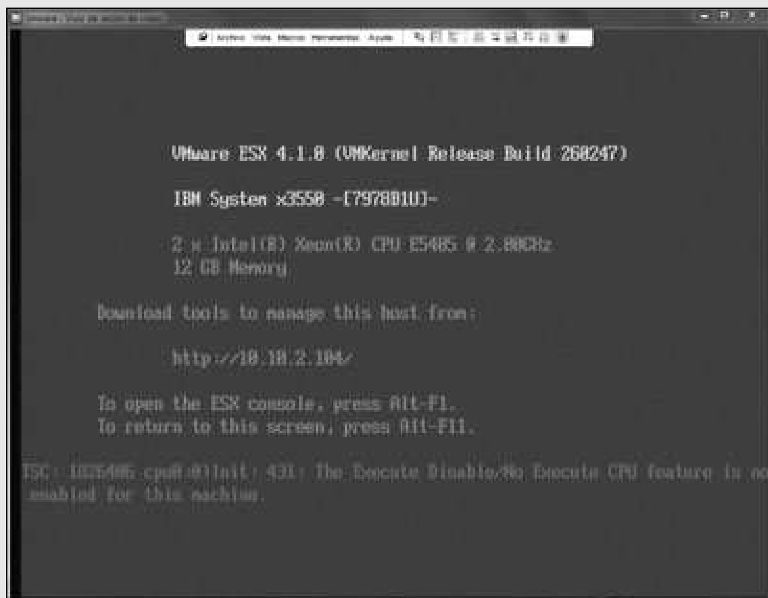
7 Elija la zona horaria y oprima **Next**. Luego puede configurar la fecha manualmente o configurar un servidor NTP para sincronizar el tiempo para el servidor.



8 Elija un password para la administración e ingréselo en **Password** y **Confirm Password**. Luego oprima **Next**. Vea el resumen y presione **Next**.



▶ 9 Al finalizar, reinicie el equipo. Luego, entre en la consola de administración de línea de comandos oprimiendo **ALT + F1** e ingresando el usuario una vez que el equipo haya terminado de iniciar.



Así, tendremos nuestro primer ESX/ESXi instalado. Del mismo modo, podremos instalar la cantidad de servidores que necesitemos. Se volverá muy engorroso administrar todos sin perder un detalle de licencias, performance y configuración, pero VMware nos da la posibilidad de manejarlos todos juntos con vCenter o vSphere.

Licenciamiento de ESX y ESXi

Entre los productos gratuitos que cada vez ganan más público, están VMware Player, VMware Server, VMware vCenter Converter y VMware vSphere Hypervisor (ESXi). Es sorprendente cómo se ha generado toda una comunidad alrededor de ellos, y es así que la Web 2.0 está empezando a cambiar la manera de pensar de las empresas. Al haber una comunidad más amplia opinando sobre un producto, se realiza más investigación, se observan más vulnerabilidades y, como resultado, obtenemos un mejor producto. La empresa así genera ingresos que aportan valor agregado a sus versiones pagas. Por el contrario, tendremos que pagar licencia por VMware Workstation, ESX y VMware Fusion.

Hay muchos plugins libres de licencias, pero las aplicaciones que más sobresalen son las que analizamos en este texto. Cuando instalemos VMware Virtual Center o

VMware vSphere, veremos que no sólo tienen una licencia para ellos, sino también para ESX/ESXi. Así, pasan a cumplir el rol de servidor de licencias para nuestra compañía. Todos los ESX y ESXi estarán apuntados hacia el virtual center para que tomen las licencias de allí. Las versiones nuevas de ESX/ESXi 4.1 vienen con un plugin para instalar, llamado VMware vSphere Licensing Report Manager. Con él podremos saber exactamente cuántas licencias hay instaladas en nuestro entorno. Otro dato importante es que nos da información sobre la cantidad de licencias que no estamos utilizando. Para los ESXi, si los activamos con licencias, tendremos otras opciones o habilidades de las que no dispondríamos si no lo hiciéramos; por ejemplo, Vmotion, HA, DRS, etc. (los veremos más adelante). Cualquier detalle sobre las licencias de nuestros productos pueden chequearse en **www.vmware.com/support/licensing**.
Si en nuestra instalación de ESX seleccionamos instalar la licencia más tarde, quedará funcionando durante un tiempo de evaluación hasta que instalemos la licencia. Para configurarla, nos conectamos a ESX, vamos a la solapa **Configuration**, elegimos **Licensed Features** e ingresamos una llave de licencia.

Cómo crear una máquina virtual

Las máquinas virtuales pueden crearse desde una migración o desde la consola de administración. Sólo debemos tener en cuenta las capacidades que necesitamos y las disponibles en el servidor físico. VMware siempre nos alertará si esto no es posible o si elegimos alguna configuración que no se pueda manejar. Hay que tener en cuenta varias opciones antes de pasar a crear la máquina virtual. Debemos pensar en configurar las placas de red virtuales, qué tamaño de disco virtual precisamos y dónde vamos a alojarlo. Otro tema son los requerimientos de memoria RAM del equipo que vamos a crear, para comparar con lo que puede ofrecernos el servidor físico, etc. No hay mejor manera de aprender sobre este tema que probando en nuestro ambiente. Más tarde, eliminaremos la máquina que no utilicemos.
La creación de una máquina virtual tanto en VMware ESX/ESXi como en las otras alternativas de virtualización es similar: hacemos clic derecho en el servidor y seguimos las opciones. A continuación, veremos paso a paso cómo crear una máquina virtual en un servidor ESX/ESXi.



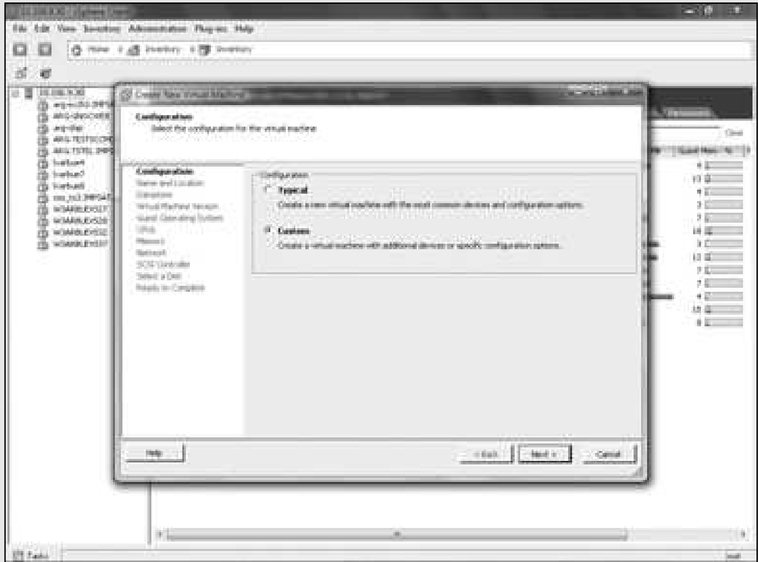
THIN PROVISIONING

Configurando los discos con Thin Provisioning, nos aseguramos de aprovechar al máximo el almacenamiento. A medida que la máquina lo necesite, se le irá otorgando más espacio en disco. Hay que tener cuidado con respecto al crecimiento. Los discos con otro formato pueden transformarse con Vmotion Storage seleccionando la opción correspondiente durante el proceso.

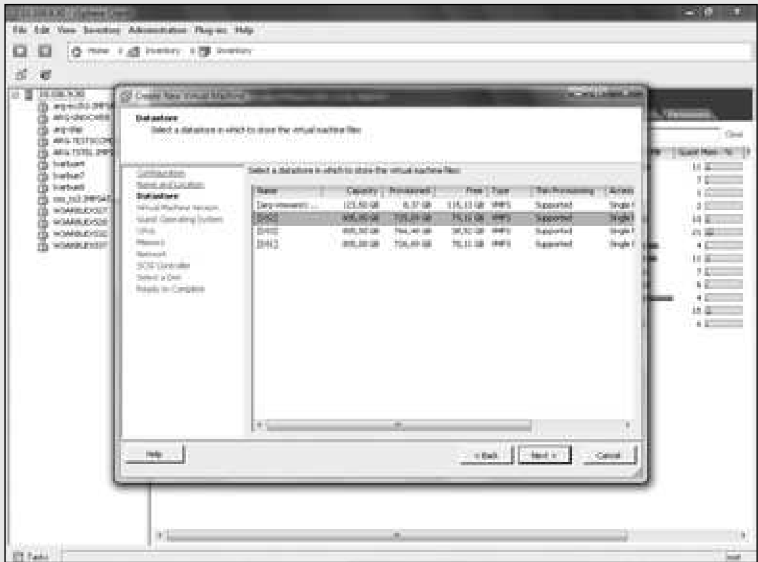
Crear una máquina virtual en ESX/ESXi

PASO A PASO

1 Abra la consola de ESX/ESXi conectándose con el cliente de escritorio o web. Ubíquese con el mouse sobre el servidor y haga clic derecho, elija **New Virtual Machine** y opte por el modo **Custom** en el paso siguiente.

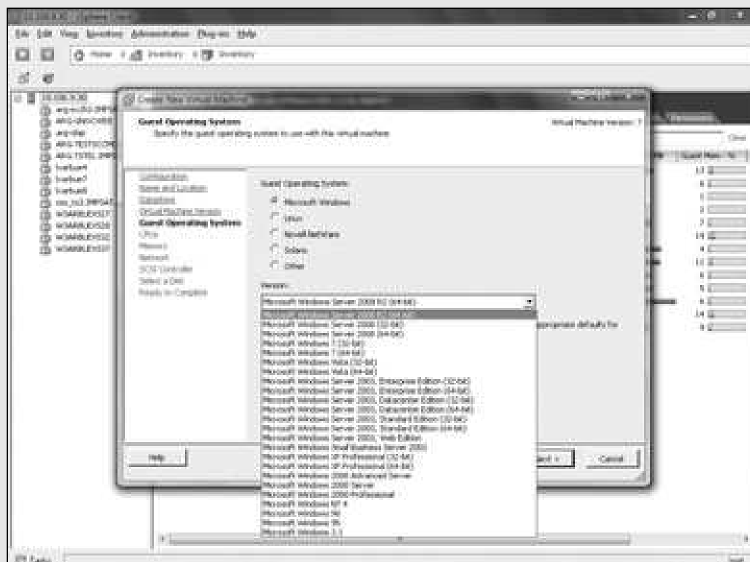


2 Elija un nombre y oprima **Next**; en el paso siguiente escoja dónde ubicará los archivos de la máquina virtual. Marque la unidad de almacenamiento correspondiente.

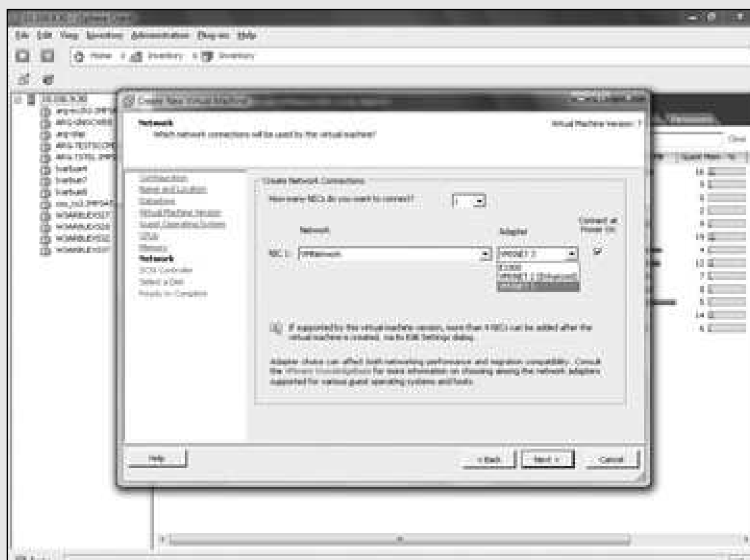


▶

3 Seleccione una versión de máquina virtual; puede ser la 4 para ESX 3.5 o anteriores, o la 7 a partir de ESX 4.0. Oprima **Next** y elija el sistema operativo por instalar del listado que aparece en pantalla.



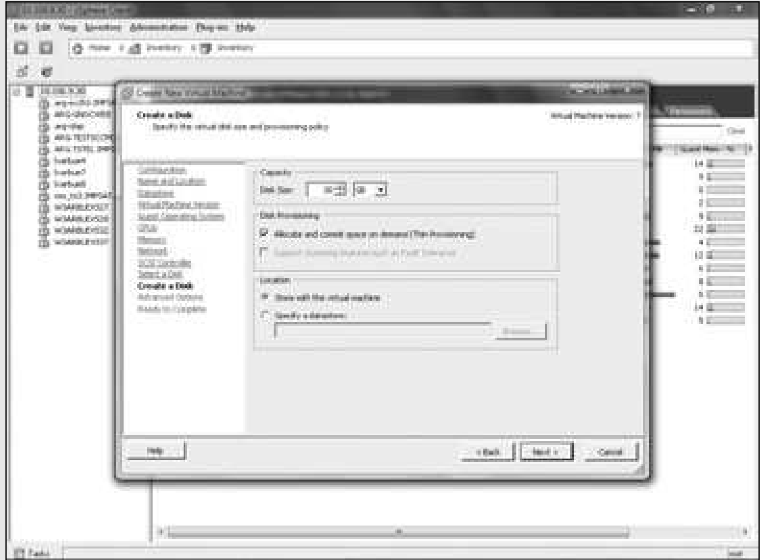
4 Indique la cantidad de microprocesadores virtuales que va a asignar, la cantidad de memoria, el tipo y la cantidad de placas de red virtuales. Elija **VMXNET3** para aprovechar todos los recursos de la virtualización.



▶

▶

5 Debe adoptar un controlador SCSI y, después, configurar un nuevo disco rígido virtual o utilizar alguno guardado. Oprima **Next**, coloque un tamaño de disco y elija una forma de entregar el espacio del disco físico. Presione **Thin Provisioning** para seguir.



6 Vea el resumen de la creación y cree la máquina virtual oprimiendo el botón **Finish**. Luego, diríjase a la consola, haga **clic derecho** en la nueva máquina virtual, elija **Power** y presione **Power on** para encenderla.



Como mencionamos en un principio, las tareas de poner en producción un servidor demandaron sólo 5 minutos, una aceleración con respecto a un servidor físico. Una vez que creamos el servidor virtual, al llegar a este punto, ya estamos en condiciones de instalar el sistema operativo para el servidor, pero ¿cómo hacerlo? Es muy sencillo. En las opciones de cualquiera de las consolas de VMware podemos mapear tanto una imagen ISO como una unidad de disco compacto para proceder a la instalación. Lo único que debemos tener en cuenta es mapearla una vez que el servidor virtual está prendido. En estos casos, nos conviene seleccionar la entrada al BIOS no bien encendemos el servidor virtual y, recién entonces, mapear el disco de instalación. Un detalle de esta configuración es que, al reiniciar el equipo virtual, el disco se desconectará automáticamente, por lo que si necesitamos seguir una instalación, deberemos volver a configurar la unidad de disco compacto. También en este capítulo veremos una manera de crear máquinas virtuales utilizando la herramienta VMware vCenter Converter. Con ella podemos migrar equipos físicos directamente a nuestras consolas de VMware, pero hay ciertos cuidados que debemos tener y los analizaremos más adelante.

Networking en VMware

Las configuraciones de red no son tan difíciles de aprender como suele pensarse. Hay que tener en cuenta ciertos conceptos que son clave para entender cómo funciona la red virtualizada. En principio, tendremos **placas de red virtuales** y **placas de red físicas**. Las físicas son las que poseen nuestros servidores VMware, son las conexiones de red de que disponemos en los servidores VMware Server, VMware Workstation y VMware ESX/ESXi. Las placas de red virtuales son las que vamos a construir a partir del software de VMware. Para cada servidor virtual, podremos crear una placa de red o varias. En la vida física, las placas de red se conectan a un puerto de un **switch físico**, en la virtual, también, estos switches van a ser virtuales. Las placas de red virtuales son asignadas desde una conexión a un **switch virtual**. Hay varias configuraciones que podemos realizar con estos conceptos. Cada placa física puede tener varios switches virtuales configurados y, a su vez, cada switch virtual puede tener varios servidores virtuales. Esto es muy común, por ejemplo, cuando nos damos cuenta de que podemos manejar las **VLANs** desde los switches virtuales.
Deberíamos ver un poco de teoría sobre redes para entender qué son las VLANs, pero trataremos de comprenderlo de la siguiente forma. Supongamos que tenemos un switch físico, y muchos puertos en cada switch, pero necesitamos agrupar las máquinas conectadas a él. Entonces, dividimos el switch en dos VLANs distintas, como si tuviéramos dos switches. En realidad, siempre será un solo switch, pero con dos grupos de máquinas distintas. Entonces, el concepto de VLANs nos dice que podemos dividir nuestra red LAN en dos. Veremos que es posible crear tantas VLANs como queramos o tantas como la cantidad de puertos nos permita. Ahora, supongamos que

tenemos dos switches y queremos que algunas máquinas conectadas a uno se agrupen con otras del otro. Entonces, lo que hacemos es compartir las VLANs. Y si tuviéramos 1000 switches y quisiéramos agrupar las máquinas conectadas a ellos en dos grupos, tendríamos dos VLANs que compartir y, así, nuestra red quedaría dividida en dos.

Simplemente, si conectáramos un puerto en trunk a nuestra tarjeta física de ESX/ESXi, podríamos manejar distintas VLANs asignándolas a diferentes switches virtuales, ya que por los puertos en estado de trunk que se configuran en los switches se pueden ver varias de las VLANs de la red. La **Figura 8** muestra un gráfico que permite esclarecer un poco esta información.

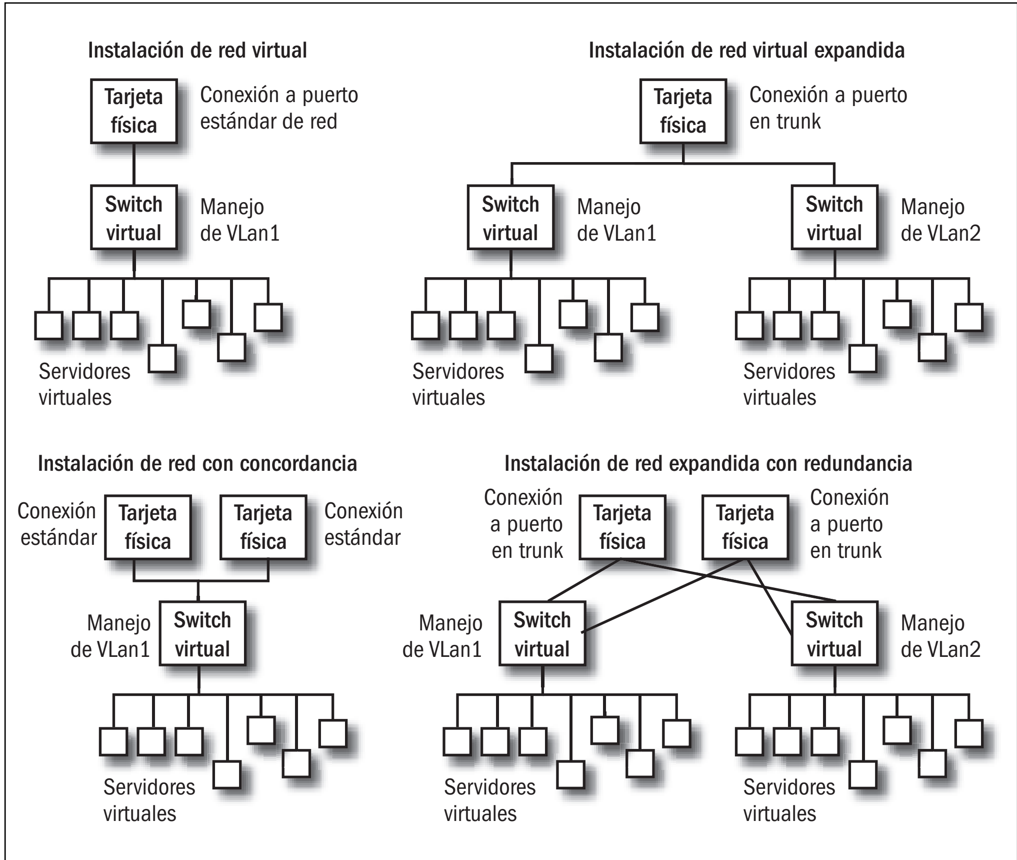


***Figura 8.** Hay por lo menos cuatro formas de conectar las redes virtuales y físicas. Cisco está desarrollando switches físicos que soporten 10 GB para modificar la gran cantidad de cables que deberíamos conectar al ESX/ESXi.*

En la instalación común de red, tendremos un cable con una VLAN conectado al servidor físico. VMware nos permite crear un switch virtual para dar soporte a más de una placa virtual y controlar el tráfico. Tendremos una sola placa de red física, un solo switch virtual y varias máquinas virtuales con sus respectivas placas

de red. En el gráfico superior derecho se observa lo que mencionamos: si conectamos un puerto en trunk a la placa física, podremos manejar una VLAN con un switch virtual y otra con otro switch virtual. Los gráficos inferiores muestran la forma de tener redundancia en la infraestructura. Al conectar dos placas de red físicas a los switches virtuales, nos estamos resguardando ante cualquier posible caída de alguna de ellas. Es un detalle más que nos permite seguir con nuestro objetivo principal: la continuidad del negocio.

Por otro lado, cuando creamos una máquina virtual, nos encontramos con distintos tipos de placas de red. Para las versiones ESX y ESXi (que son las que nos interesan), tendremos cuatro tipos principales en la versión 4.1. El primero es el **Flexible**, que es el que viene predeterminado. La tarjeta es reconocida por el sistema operativo como **VLance** o **VMXNET** dependiendo del controlador que se haya instalado; puede reconocerse de distinta forma según el sistema operativo que utilicemos. Por ejemplo, en sistemas Windows 2000, es reconocido como VMware Accelerated AMD PCNet Adapter. El otro tipo que podemos encontrar es el **E1000**, una versión emulada del controlador Intel 82545EM Gigabit Ethernet. Varios sistemas operativos incluyen un controlador para esta placa, por lo que no tendremos problemas en utilizarla. Por ejemplo, es compatible con Linux versiones 2.4.19 en adelante, Windows XP Profesional x64 en adelante y Windows Server 2003 x86 en adelante.

El tercer tipo de placas de red virtuales que podemos utilizar es el **VMXNET2(mejorado)**, una placa optimizada para ambientes virtuales. Como los sistemas operativos no tienen conocimiento de esta placa, hay que tener instaladas las opciones de VMtool para utilizarla. Este tipo de placa virtual viene en sistemas ESX/ESXi 3.5 en adelante y es soportado por un número limitado de sistemas operativos, que mencionamos a continuación:

- Microsoft Windows Server 2003 Enterprise y Datacenter (32 y 64 bits)
- Microsoft Windows XP (32 bits)
- Red Hat Enterprise Linux 5.0 (32 y 64 bits)
- SUSE Linux Enterprise Server 10 (32 y 64 bits)
- Red Hat Enterprise Linux 4.0 (64 bits)
- Ubuntu Linux (64 bits)



PUERTO TRUNK

Para compartir las VLANs, lo realizamos a través de switches. Éstos utilizan un puerto especial. Se dice que el puerto está en trunk cuando por un solo cable es posible ver todas las VLANs. Estos puertos son reconocidos de forma especial en cada switch y son administrados automáticamente por ellos. Es así como, desde otro switch, podemos ver las VLANs de otro equipo.

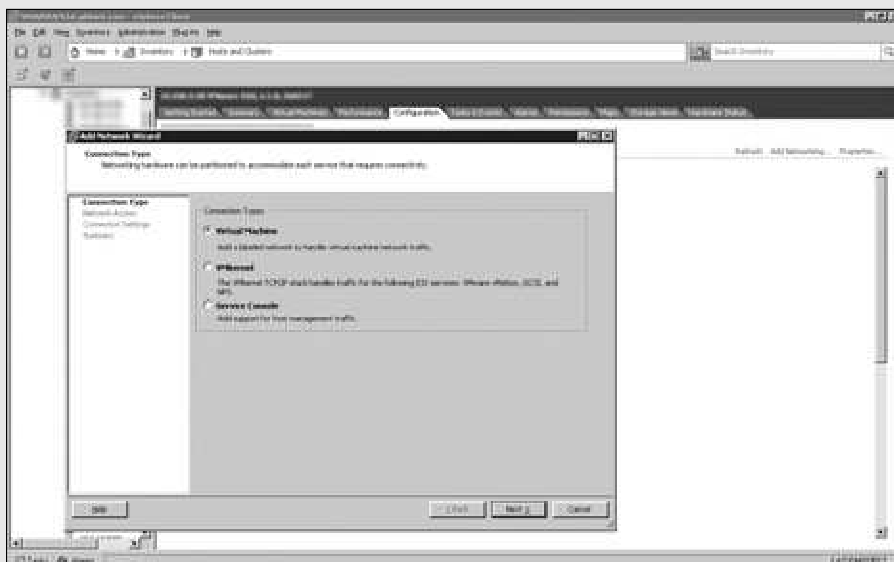
Por último, podemos encontrar el tipo de placa más recomendado, el **VMXNET3**, completamente pensado y creado para plataformas virtuales. No tiene relación con los antiguos VMXNET, y entre sus diversas características nuevas, trae soporte para IPv6. Funciona sólo en máquinas virtuales versión 7 que únicamente pueden ser creadas con vSphere 4.1. Los sistemas operativos compatibles son:

- Microsoft Windows Server 2003, XP y 2008 (32 y 64 bits)
- Red Hat Enterprise Linux 5.0 en adelante (32 y 64 bits)
- SUSE Linux Enterprise Server 10 en adelante (32 y 64 bits)
- Asianux 3 en adelante (32 y 64 bits)
- Debian 4/Ubuntu 7.04 en adelante (32 y 64 bits)
- Oracle Solaris 10 U4 en adelante (32 y 64 bits)

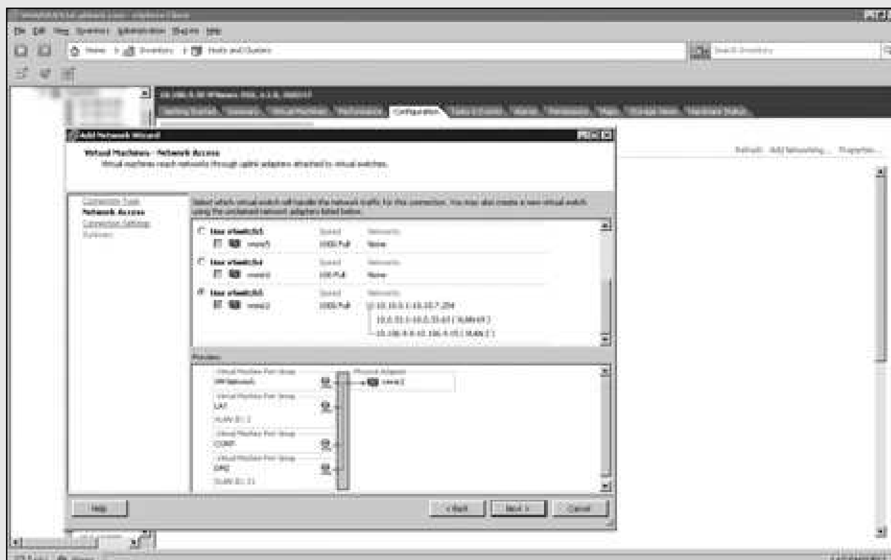
Estas últimas, las VMXNET3, llegan a darnos velocidades de hasta 10 Gb en ambientes virtuales, aunque la conexión física sea de 1 GB. A continuación, veremos cómo crear un nuevo switch virtual a partir de una placa física conectada a un puerto trunk.

Crear un switch virtual a partir de un puerto trunk — PASO A PASO

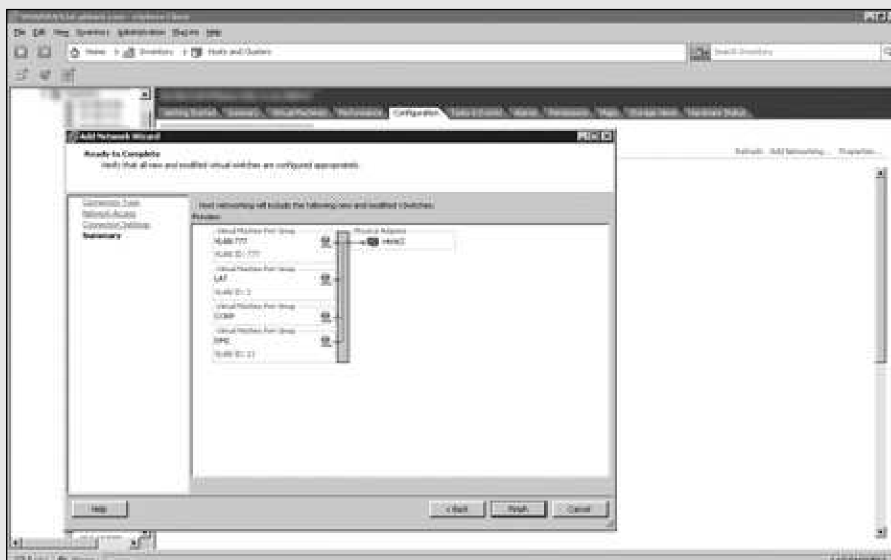
1 Conéctese a la consola de **VMware vSphere/Virtual Center**. Ubíquese en el servidor ESX/ESXi y vaya hasta la solapa **Configuration**. Allí, en la opción **Networking** del menú de la derecha, haga clic en el link denominado **Add Networking**, arriba a la izquierda. Para las máquinas virtuales elija el tipo de conexión conocido como **Virtual Machine**.



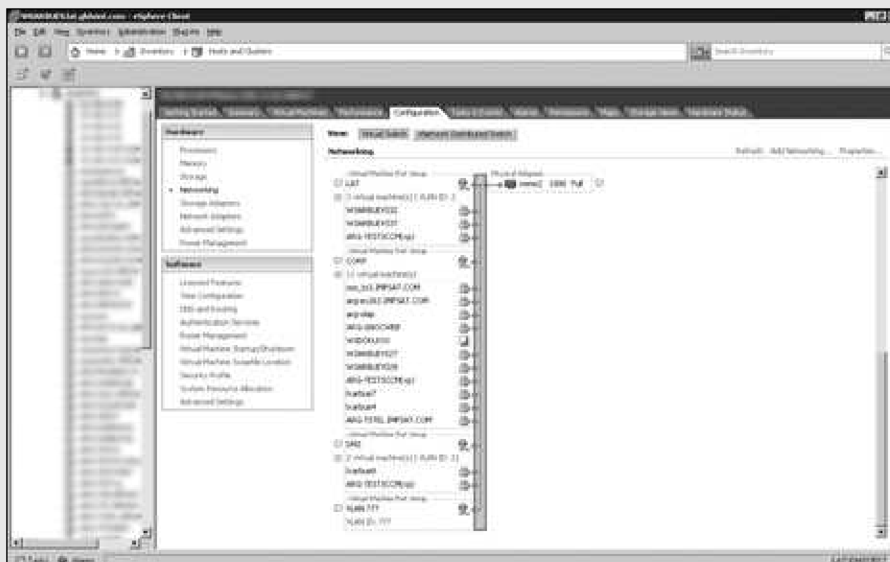
2 Seleccione la placa de red física en donde esté conectado el puerto **trunk**. Lo distinguirá por tener un listado de redes disponibles. Elija una de las **VLANs** disponibles; recuerde el número.



3 En este paso deberá escribir un nombre para el switch virtual y configurar el número de VLAN elegido en el campo **VLAN ID**. Oprima el botón **Next**, vea el resumen de la operación y presione sobre **Finish**.



▶ **4** Corrobore la configuración del switch en el gráfico de **Networking**; el adaptador debe corresponder con la velocidad y VLAN elegida.



Hemos visto en el paso 1 que, al elegir las conexiones, se nos presentan tres posibilidades. La que escogimos en nuestro ejemplo se denomina **Virtual Machine**; se trata de una opción especial para proceder a crear un switch virtual que funcione en forma dedicada a brindar conexión a las máquinas virtuales correspondientes. Debemos tener en cuenta que cuando creamos una máquina virtual, sólo podemos elegir switches virtuales creados de esta forma; no es posible elegir los otros. El tipo llamado **Vmkernel** es usado, exclusivamente, por ESX para realizar el tráfico de servicios del tipo vMotion, iSCI y NFS. Por último, el tipo **Service Console** es exclusivo para realizar la conexión con la consola de servicios.Cuando instalamos ESX/ESXi, también instalamos un switch de este tipo; sólo si creamos redundancia a nivel de red, tendremos que crear otro.

Comandos básicos para la administración de ESX

Podemos administrar cada ESX desde la consola gráfica o desde la consola de líneas de comando. Como el sistema operativo es un Linux remodelado, contaremos con todos los comandos Linux que conocemos, y VMware agregará 250 comandos propios, programas ya compilados para realizar ciertas acciones. Estos comandos se administran conectándonos al **Service Console** o vía SSH, con aplicaciones tipo **PuTTy**. Algunos de los comandos más utilizados son:

USO	LÍNEA DE COMANDO
Entrar a modo de mantenimiento (maintenance mode)	vimsh -n -e /hostsvc/maintenance_mode_enter
Salir del modo de mantenimiento	vimsh -n -e /hostsvc/maintenance_mode_exit
Abrir temporalmente todos los puertos del firewall del ESX	esxcfg-firewall -allowIncoming
	esxcfg-firewall -allowOutgoing
Habilitar servicios en el firewall	esxcfg-firewall -e sshClient
	esxcfg-firewall -e ntpClient
	esxcfg-firewall -e snmpd
Listar los switches virtuales	esxcfg-vswitch -l
Listar las placas de red	esxcfg-nics -l

Tabla 3. *Comandos más utilizados en la consola de texto.*

En todos los comandos, podemos asignar la opción **–h** para ver la ayuda correspondiente y otras opciones de que disponen. Esta posibilidad de correr scripts desde Service Console directamente sobre ESX deja de lado la migración que se está realizando a ESXi. Los administradores de seguridad tienen menos para controlar, pero los del ambiente virtual que ya han adquirido experiencia tienen algo nuevo que aprender. Las herramientas que podemos utilizar en vez de Service Console son **vCLI**, **PowerCLI** y **vMA**. La primera es una consola que funciona sobre Windows o Linux. Se parece mucho al Service Console con scripts realizados en lenguaje Perl. Muchos de los comandos utilizados en el Service Console se mantienen por compatibilidad, pero van a desaparecer tarde o temprano. Podemos desarrollar nuestros propios scripts en Perl si tenemos conocimientos sobre el tema. Con vSphere SDK para Perl, podemos hacer cualquier cosa que se nos ocurra. vCLI cuenta con casi 30 scripts completos; por el contrario, PowerCLI suma 160 cmdlets para administrar VMware ESX desde una consola Power Shell de Microsoft (los cmdlets son scripts compilados para utilizar en Power Shell). Sin dudas, vMA es la más potente de todas las opciones. Se puede bajar muy fácilmente porque es un Virtual Appliance (máquinas virtuales que podemos descargar desde Internet, veremos los detalles al finalizar el capítulo) que cuenta con CentOS 5.2, vCLI, vSphere SDK for Perl, CIM, Java JRE y vSphere SDK for Java. Podemos descargarla desde la dirección: **www.vmware.com/support/developer/vima**.

Consola gráfica de administración ESX/ESXi

La consola gráfica es otra forma de administración del ESX, y permite hacer muchas cosas que realizamos desde la línea de comandos, pero gráficamente. Se compone de tres grandes grupos de información: por un lado, el servidor ESX y las máquinas virtuales; por otro, los detalles del servidor ESX y de cada máquina virtual; y más abajo, la lista de tareas que se van realizando a medida que van pasando. No importa el usuario, se informan todas las tareas efectuadas en el servidor: una a la

izquierda, donde se encuentra el árbol de clusters y máquinas virtuales; y otra a la derecha, en la que se muestran los detalles de donde estemos parados, ya sea del cluster, de cada ESX o de máquinas virtuales.

Sectores de la consola gráfica

GUÍA VISUAL

❶ **Servidor ESX:** en esta sección se identifica por su dirección IP al servidor ESX que alojará los distintos servidores virtuales.

❷ **Servidores virtuales:** aquí se muestra el detalle correspondiente a los distintos servidores virtuales que tenemos disponibles.

❸ **Detalles:** en la parte central de la pantalla, veremos distintas solapas con información detallada sobre configuración, recursos, rendimiento, usuarios, eventos y permisos del servidor ESX. Posicionándonos en cada servidor virtual, accederemos a sus características.

❹ **Tareas:** en el sector inferior de la ventana podemos observar las tareas a medida que vayan sucediendo, de manera que obtendremos información en tiempo real.

Debemos saber que la consola mostrada en la Guía visual anterior pertenece al cliente de escritorio para VMware llamado vSphere. Tengamos en cuenta que el cliente que viene con ESX es muy similar.

CÓMO VIRTUALIZAR UN SERVIDOR

Ya vimos de qué manera instalar la infraestructura necesaria para implementar la virtualización, pero seguimos teniendo muchos servidores físicos brindando servicios críticos en la empresa. A continuación aprenderemos a transformar estos servidores físicos en virtuales sin perder datos, permisos ni configuraciones, y manteniendo la continuidad del negocio y realizando los cambios en el menor tiempo posible. Así, podremos optimizar nuestra infraestructura en cuanto a consumo de hardware, ahorro de recursos, agilidad en la administración, y posibilidad de expansión y actualización.

Detalles antes de migrar

Hace tiempo, era impensable pasar un servidor físico a uno virtual; directamente, nadie hablaba sobre eso. Hoy en día, es un trabajo en gran auge. En el informe de la empresa Gartner sobre las visiones de los principales CEOs de la industria, además de ubicar a la virtualización en el primer puesto, si buscamos los aspectos más relevantes dentro de este tema, el hecho de convertir servidores físicos en virtuales es el más notorio, y en las empresas no hay personal capacitado para realizar esta tarea. Antes era muy complicado hacerlo y ocurrían muchas fallas, pero con la nueva versión de VMware Converter, ya se repararon muchos de los errores que se presentaban en este procedimiento, haciéndolo más confiable. Pero esta acción no sólo requiere saber utilizar la herramienta mencionada y seguir un par de pasos.

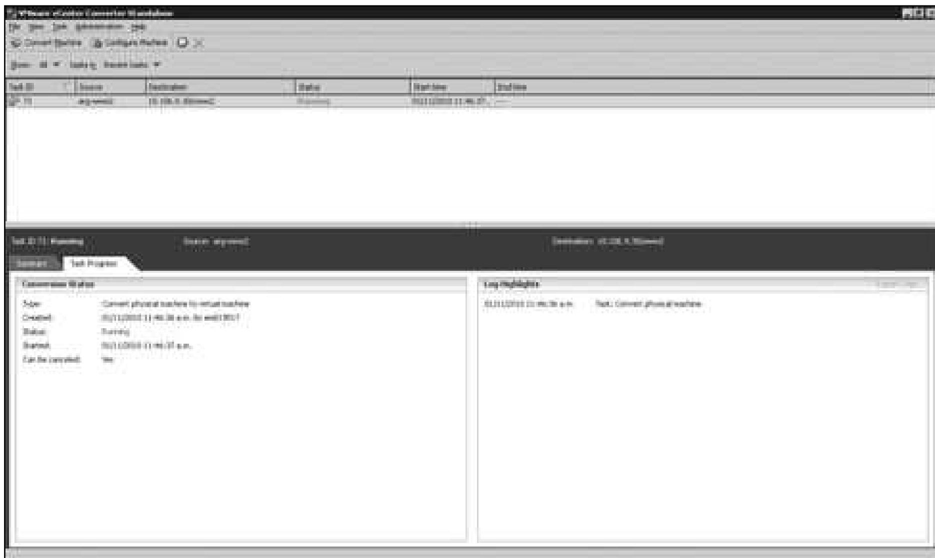


Figura 9. *La consola de VMware Converter es muy sencilla: sólo informa las tareas que se realizaron, las que están en curso y las que fallaron. Es posible virtualizar más de un servidor al mismo tiempo, lo que acelera la normalización de equipos.*

Hay varios aspectos para tener en cuenta. Por ejemplo, si migramos un servidor web que contiene 20 sitios productivos en los cuales se conectan usuarios de la empresa, más otro grupo de usuarios externos a ella, de donde se obtienen informes porque posee un Report Services instalado y, a la vez, se utiliza como servidor FTP. No sólo es cuestión de saber utilizar la herramienta, sino que necesitamos administrar muchas tareas, coordinar acciones con numerosos usuarios y efectuar acciones fuera de horario. Todo esto, sin mencionar las configuraciones de red que se pierden al virtualizar. El proceso deja una copia del servidor, pero los controladores de red se reemplazan por los virtuales, con lo cual se pierden las configuraciones de IP, MAC Address y rutas estáticas que podemos llegar a tener. También pueden tener acceso a redes a las que nuestro ESX no llega, o puede ser que haya configuradas varias direcciones IP. Al migrar un servidor físico a uno virtual, es preciso tener mucho cuidado en las configuraciones de red. Principalmente, en la cantidad de IP, la tabla de ruteo, las reglas en el firewall y al copiar la dirección MAC del controlador.
Si tenemos un servidor de aplicaciones, la sincronización de datos es crítica. Puede ser que nosotros estemos realizando la copia del servidor en línea y que, mientras hacemos el cambio de físico a virtual, alguien actualice una carpeta de la aplicación. En ese caso se produce pérdida de información. Lo recomendable es fijar reuniones con todos los especialistas, usuarios y administradores que tienen incidencia en el servidor por virtualizar, e incluirlos para que nada falle. Si el usuario está avisado, no debería de actualizar una carpeta durante el rango horario de migración.
El problema es exponencial al migrar un servidor de base de datos. Hoy se habla de almacenamientos de TB de información. ¿Qué sucede una vez que realizamos la copia virtual? El segundo siguiente, la información entre los dos servidores es diferente. En este caso, lo recomendable es planificar un horario de migración, bajar las bases de datos y virtualizar el servidor. Una vez que se hizo la copia, se verifica su funcionamiento y se ponen en línea las bases de datos.

Descripción del procedimiento

El procedimiento de migración es sencillo; lleva tiempo pero es simple. Como primera medida, debemos generar un plan. Una práctica recomendable es virtualizar el equipo previamente, ponerlo en un ambiente de testing y verificar que funcione como corresponde. Este tema lo veremos más adelante, pero hacer la copia no interfiere en las tareas cotidianas. Si el sistema está basado en Windows 2000 o anterior, necesitará un reinicio. Sólo se instala un agente de VMware Converter y se comienza a copiar la información; el destino de la copia puede ser cualquier ambiente de VMware: Player, Workstation, Server o ESX/ESXi. Lo recomendable es utilizar la versión Server, y no comprometernos con servidores ESX/ESXi.
Luego de la prueba y el armado del plan, comenzamos a contactar a los usuarios, vemos los tiempos posibles y definimos una agenda. Conviene anotar y tener en cuenta todas

las posibilidades de pérdida de datos, de pérdida de sincronización o configuraciones, para estar al tanto e ir directamente al problema si debemos realizar tareas de troubleshooting. Durante la fase de virtualización, sólo debemos utilizar VMware Converter desde el server destino o desde uno que esté en el medio de los dos. La aplicación instalará un agente en el servidor físico por virtualizar y comenzará a copiar.

Debemos saber cuál es el mejor momento para hacer el cambio del servidor físico por el virtual e implementarlo. Lo recomendable es tener una consola IP conectada al servidor físico, para no perder conexión cuando demos de baja la placa de red. No vamos a apagarlo si lo tenemos así conectado. Lo correcto es deshabilitar la placa de red del servidor físico y habilitar la placa del servidor virtual. Luego, estaremos en condiciones de decir que el servidor físico ya no lo es más, y que ahora es virtual. Entonces, procedemos a apagar el hardware físico no usado y a reciclarlo.

Migración de un servidor físico a uno virtual

Como detallamos antes, el procedimiento consiste en utilizar VMware Converter, que copiará el agente por nosotros, mandará a reiniciar el servidor si es necesario y comenzará el proceso. Luego, para finalizar, hacemos el cambio. A continuación, veremos un procedimiento para que, una vez que tengamos todo planeado, podamos virtualizar.

■ Convertir un servidor físico en virtual — PASO A PASO

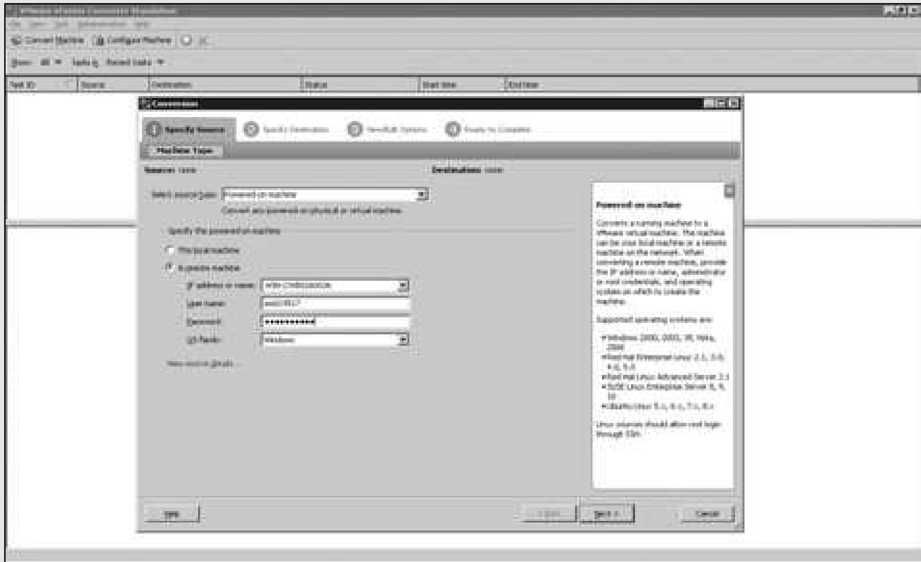
1 Como primer paso, baje VMware Converter e instálelo en cualquier servidor o PC. Puede obtenerlo de la dirección: **www.vmware.com/products/converter**.



►

▶

2 Ejecute la aplicación en un equipo. Elija **Powered-on machine** en las opciones **Select source type**. Marque **A remote machine** y complete la información.

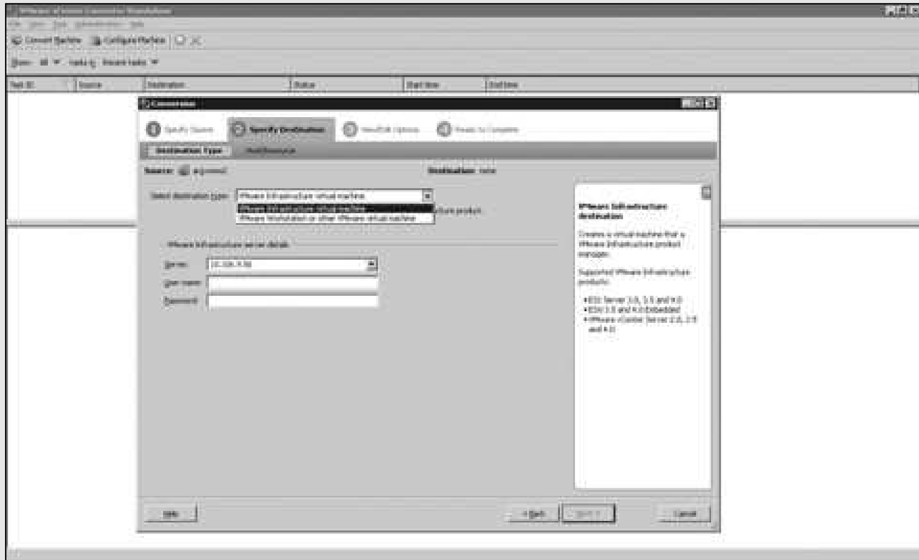


3 Seleccione la opción **I will manualy uninstall the files later** y oprima la opción denominada **Yes** para iniciar la instalación del cliente.



▶

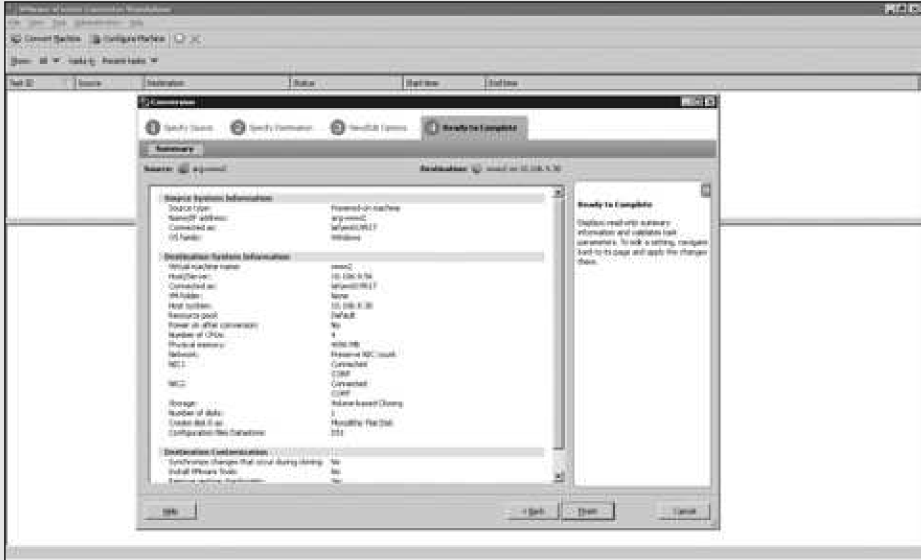
4 Para continuar, deberá escoger el destino, si es un **VMware Infrastructure** (ESX) u otro tipo de aplicación, como por ejemplo **VMware Workstation**. Posteriormente, complete los datos debajo y oprima el botón llamado **Next**.



5 Seleccione el storage de destino, y acto seguido, complete los datos de versión y nombre. Oprima el botón denominado **Next**.



6 Vea el resumen, oprima **Next** y presione el botón **Finish** para comenzar a virtualizar. Verifique el avance y compruebe si la tarea se completa sin errores.



La instalación de VMware Converter es muy sencilla y sólo requiere unos pocos pasos. No tendremos complicaciones e, incluso, podremos correr el software en una máquina no muy grande. En el paso 2 del procedimiento anterior, donde indicamos elegir **Power-on machine**, también tendremos la opción de migrar el servidor cuando está apagado. Otra posibilidad es migrar un servidor desde algún otro formato de máquinas virtuales, desde Microsoft Virtual Server 2005, desde Hyper-v, desde VMware Workstation o Player (para pasarlo a un ambiente ESX), y otros formatos. En el paso 3 también podemos utilizar la opción automática, pero si la virtualización falla por algún motivo, tendremos que instalar el cliente otra vez, y esto lleva unos minutos que lograremos ahorrar si elegimos el modo manual. El destino de la máquina por convertir puede ser un ambiente ESX o, también, VMware Workstation o VMware Player.



APAGAR LAS CONEXIONES DE RED

Debemos tener en cuenta que una vez que terminemos la copia, lo recomendable es encender el servidor sin conexión a la red, configurar las placas de red tal como estaba el servidor físico, verificar aplicaciones y preparar cualquier otra cuestión con la red apagada. Esto es fundamental para no interferir con el trabajo en la red del servidor que aún es físico.

VIRTUAL CENTER

Ya sabemos cómo administrar un servidor ESX, pero ¿qué pasa si tenemos dos, tres o diez? ¿Cómo los administramos? La solución de VMware para este caso es **Virtual Center**. Con esta herramienta podremos centralizar toda la administración de varios servidores ESX en una sola consola, compartir recursos y estadísticas, y mover máquinas virtuales entre los distintos servidores con mínima pérdida de datos. Veremos una introducción a este tema, conoceremos cómo implementarlo y aprenderemos la manera de clonar servidores.

Descripción de Virtual Center

Virtual Center es, sin dudas, una de las mejores soluciones para centralizar nuestra administración del ambiente virtual. No sólo permite centralizar la administración, sino que también ofrece la automatización de ciertas configuraciones, optimización de recursos y una gran capacidad para incrementar la alta disponibilidad de nuestros servidores. Entre los mejores beneficios que brinda, encontramos que nos permite alinearnos con prioridades de negocios predefinidas para volcar los recursos de hardware hacia donde lo demande la empresa, en el momento en que lo necesite, utilizando VMware DRS. Además, podremos migrar máquinas entre distintos nodos ESX sin tener ninguna pérdida de datos, sin tener ni siquiera un reinicio y sin necesidad de ningún tipo de mantenimiento mediante VMware Vmotion. También independiza las aplicaciones del hardware y de las operaciones de sistemas utilizando VMware HA. Para activar estas características de HA y DRS, y hacer Vmotion entre los distintos nodos que queremos administrar con Virtual Center, éstos deben tener las mismas características de hardware e idénticas conexiones de red que compartir. A su vez, deben compartir una unidad de almacenamiento. Los archivos de los servidores virtuales se almacenarán en esa unidad compartida, y sólo se tomarán de los nodos los recursos de microprocesador y memoria RAM. Podemos administrar varios ESX, tener varios clusters administrados y, en cada uno de ellos, tendremos equipos con las mismas características, como dijimos anteriormente. Virtual Center incluye una característica de HA que permite que nuestros equipos tengan el menor tiempo de bajada posible. Si se cae un nodo, si se rompe o deja de funcionar, las máquinas virtuales que aloja se reiniciarán y aparecerán distribuidas entre los otros nodos que conformen el cluster; de ahí que los nodos de un mismo cluster deban ser iguales. Para acceder a la consola, nos conectamos con el **Virtual Center Client**, al igual que lo hacíamos en un nodo ESX, pero esta vez, al VMware Virtual Center. Para acceder, debemos ser usuarios administradores del servidor o podemos administrar los permisos de forma más avanzada integrando el Virtual Center con Active Directory. Tendremos gran velocidad a la hora de poner productivo un servidor, ya que podremos realizar templates (plantillas de servidores), clonar (copiar

servidores) y crear un servidor virtual con unos pocos clics. Mediante una API de programación llamada **VMware Infrastructure SDK**, es posible integrar aplicaciones y crear las nuestras mediante el consumo de web services (servicios web).

Detalles de su implementación

Para la implementación podemos usar un servidor virtual o uno físico. Como vimos, es posible configurar el Virtual Center como central de licencias; así, si se llega a romper el servidor, los ESX quedan con licencia de prueba por determinados días. Podemos tener como resguardo un servidor fuera de la **granja virtual**, que sea físico, y más tarde, virtualizarlo por si es necesario. Entonces, tendremos el físico funcionando y el virtual apagado. Virtual Center trabaja con dos bases de datos: una para la administración de los servidores virtuales y otra para la administración de los parches. Debemos tener espacio para estas bases en las unidades de almacenamiento; pueden instalarse en el mismo servidor en donde está Virtual Center o en otro. En caso de tener que actualizar, podemos crear backups y toda una serie de tareas de mantenimiento para el servidor, pero la experiencia dice que es más fácil hacer borrón y cuenta nueva instalando todo desde cero. Sólo tenemos que agregar los nodos otra vez y configurar algunos aspectos, pero la instalación será más limpia y funcionará mucho mejor. Así nos ahorraremos gran cantidad de problemas de instalación de plugins, ya que únicamente tenemos que habilitarlos de nuevo. Si hacemos sólo una actualización sobre el Virtual Center ya instalado, en ocasiones los plugins no funcionan correctamente. Debemos tener un storage compartido para los nodos ESX, que puede estar conectado vía un canal de fibra o iSCI.

Particularidades del storage compartido

El storage compartido debe ser compatible con los productos de VMware, lo que se avala en la planilla de compatibilidad. Si esto no es así, es posible que, luego de instalar todo y configurarlo correctamente, surjan fallas que aparezcan y desaparezcan. Un problema muy común en estas circunstancias es que las LUNs (las unidades de disco que nos dan los administradores de storage) se desconecten sin razón alguna. Como primer paso, entonces, al momento de definir un almacenamiento compartido, hay que revisar el sitio de compatibilidad. Cuando ya lo hayamos definido, conectado y configurado en la consola del storage, lo configuramos en los nodos ESX. Debemos configurar las mismas LUNs para los mismos nodos en el mismo cluster. Podemos llegar a configurar más de una LUN para distintos clusters y, luego, al crear un servidor virtual, elegir dónde almacenarlo. En el caso de una conexión de fibra, sólo debemos conectar los cables al equipo e ir a la consola de administración, en la solapa de configuración buscar **Storage** y allí oprimir **Rescan All**, como vemos en la **Figura 10**.

Figura 10. *Podemos volver a escanear todas las unidades conectadas al equipo. Una vez realizado el scan, la nueva conexión figurará en la consola.*

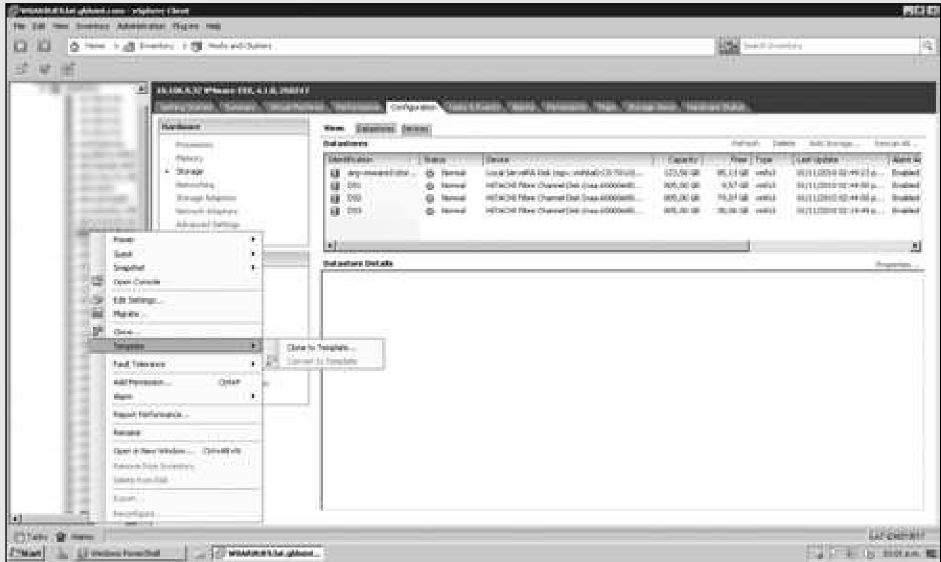
Cómo crear un template

La creación de templates es muy fácil de realizar y nos permite tener, en minutos, un servidor productivo basándonos en la configuración de otro servidor previo. Las acciones de clonar y hacer un template van de la mano. Clonar es la copia exacta de un servidor en funcionamiento o apagado; la replicación es precisa. Si lo creamos y enseguida encendemos el servidor en la red, puede llegar a haber conflictos de red, ya que ambos tendrán las mismas configuraciones, el mismo nombre de red, etc. Para que esto no ocurra, se utiliza una herramienta llamada **newsid**. El número **sid** es unívoco y corresponde a un servidor en el dominio. Su función es crear un nuevo número para que no interfiera con el anterior y cambiarle el nombre de red.

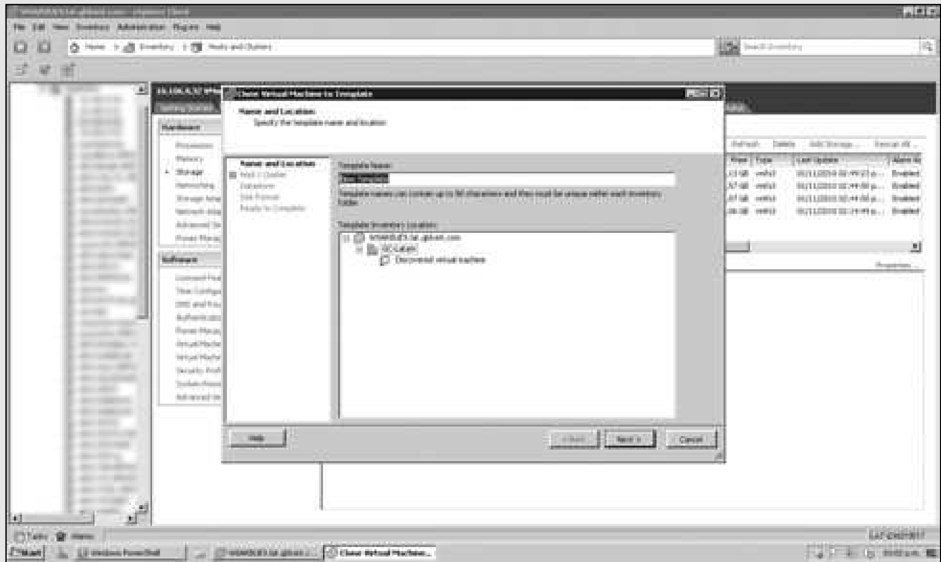
Entonces, tenemos dos casos por analizar. En el primero supongamos que hacemos tan sólo una clonación, por lo que debemos desconectar la red virtual, correr esa herramienta y, luego, conectarla a la red y terminar la configuración. Otra forma mucho más práctica es crear un template, una plantilla, que no es más que un servidor clonado que se guarda apagado en nuestra granja, y luego, desde él se crean más copias, para generar así servidores nuevos a partir de esa plantilla. Lo que conviene hacer en este caso, al crear un template, es abarcar todas las posibilidades de configuraciones, correr la herramienta newsid y, al momento del reinicio, dejarlo apagado y crear el template en ese instante. Luego, cuando hacemos un **deploy** (una copia del template), nos ahorraremos muchos pasos en el proceso. De esta manera, podríamos tener templates de distintos sistemas operativos: uno de Windows Server 2003 estándar, otro de 2008 Enterprise, etcétera, cada uno, dormido hasta que necesitemos una copia.

Crear un template a partir de un server — PASO A PASO

1 En la consola, ubíquese sobre el servidor virtual con el que quiera crear el template. Haga clic derecho y elija **Template/Clone to Template**.

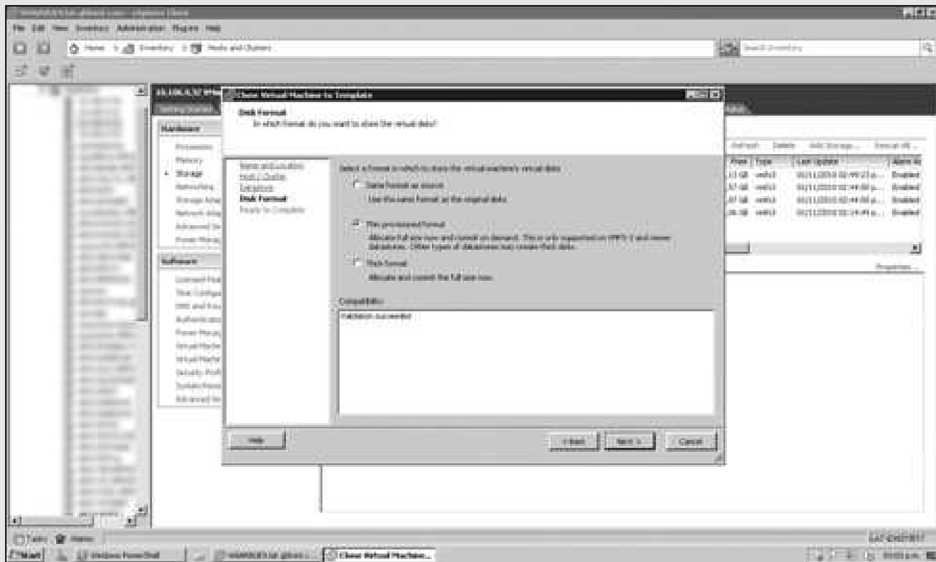


2 Elija un nombre para el template, el **datacenter** destino y oprima **Next**. Luego, seleccione el **cluster** destino y presione la opción llamada **Next**. A continuación, escoja el storage destino y pulse **Next**.

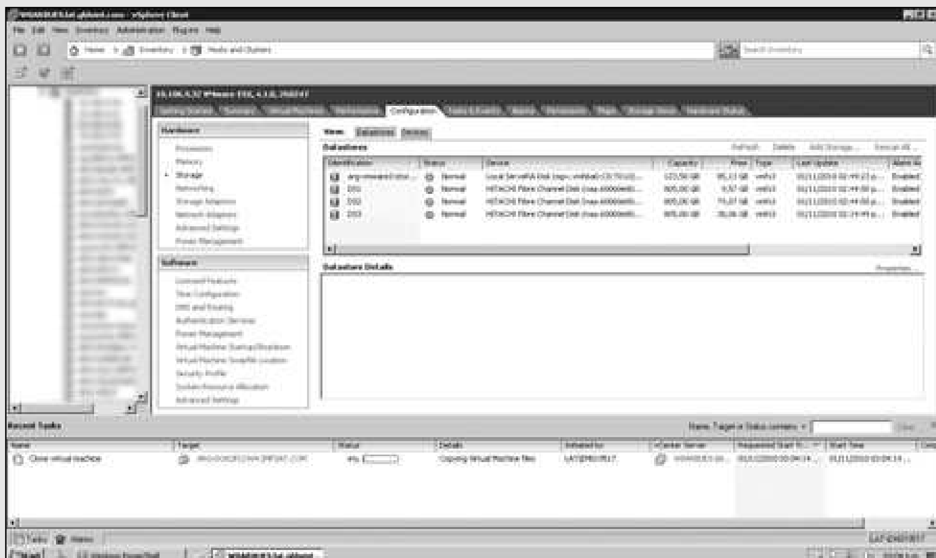


▶

3 Para continuar, debe seleccionar el formato de disco, para lo cual tiene que elegir la opción denominada **Thin provisioned format** y, posteriormente, oprimir el botón **Next**. Vea el resumen y pulse **Finish**.



4 Verifique en la consola, en las tareas que figuran abajo, que la clonación haya comenzado. Analice la evolución y suspéndala si tarda más de cuatro horas, porque significa que algún error no permite que se ejecute la operación.



VIRTUAL APPLIANCE

Explicaremos a continuación cuál es la forma más veloz y sencilla de poner en funcionamiento sistemas que pueden dar servicio rápidamente en una empresa. Con nuestra infraestructura de Virtual Center trabajando, podremos desplegar estos sistemas creados por miles de personas alrededor del mundo. Explicaremos en esta sección de qué se trata este tema y veremos cómo instalarlos en nuestra empresa.

Qué son los virtual appliance

Los virtual appliance son instalaciones de **servidores predefinidos**. Es como crear un servidor virtual, configurarlo para que brinde un servicio de MsSQL y dejarlo en la Web para que cualquiera pueda utilizarlo. Hay algunos que son pagos, mientras que otros son de libre descarga. En **VA Marketplace** hay miles de servidores virtuales listos para usar. En muchos casos, debemos bajarlos a nuestra infraestructura de Virtual Center y encenderlos. Casi todos brindan servicios web, de modo que, para administrarlos, tenemos que acceder al sitio web que estará en nuestra red, y listo. Algunos ejemplos son wikis, sistemas para crear blogs, intranets, monitoreos de red y de servidores, etc. Los virtual appliance se distribuyen con un formato llamado **.OVF** (*Open Virtualization Format*), un sistema de distribución de archivos comprimidos que es un estándar para las máquinas virtuales. Este estándar está avalado por las principales compañías del mercado, como DELL, HP, IBM, Microsoft, VMware y XenSource (Citrix).

Cómo instalar un virtual appliance

Podemos tener varios virtual appliance instalados en la empresa, pero siempre debemos asegurarnos de que provengan de fuentes confiables, y hacer una pequeña investigación en Internet para conocer opiniones y ver calificaciones. Es muy aconsejable realizar esta tarea antes de echar mano a una distribución nueva. La instalación no requiere tener muchos conocimientos: es rápida, sencilla y segura. Para lograrlo, debemos realizar el procedimiento que se indica a continuación:

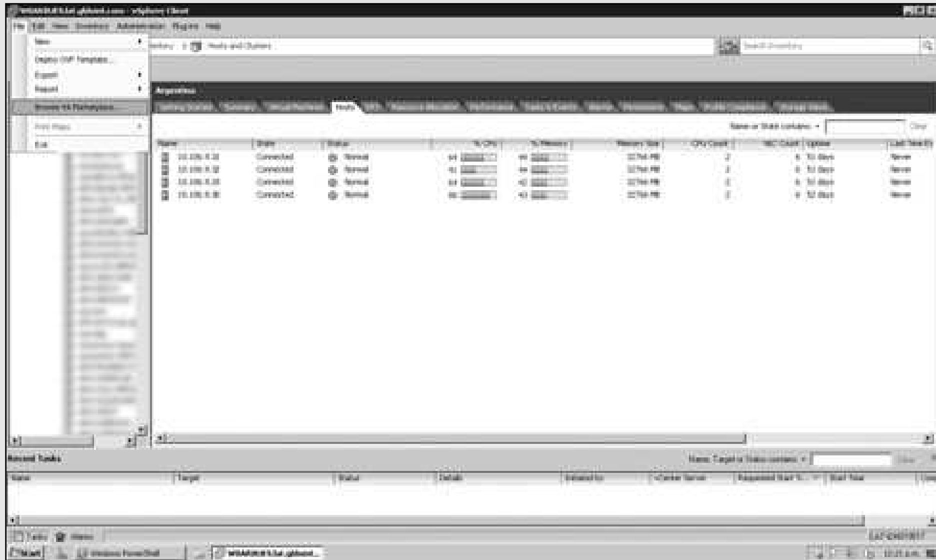


TEMPLATES

Los templates son plantillas de servidores. Cuando queramos hacer un servidor de ciertas características (por ejemplo, servidores de SQL 2008 o Apache), sólo debemos realizarlo una vez. Luego, creamos un template y hacemos un despliegue de él cuando necesitemos uno nuevo. Con tan sólo unas correcciones, tendremos el sistema funcionando.

Cómo instalar un virtual appliance — PASO A PASO

1 En primer lugar deberá ingresar a la consola; una vez que se encuentre en ella diríjase al menú **File/Browse VA Marketplace**.

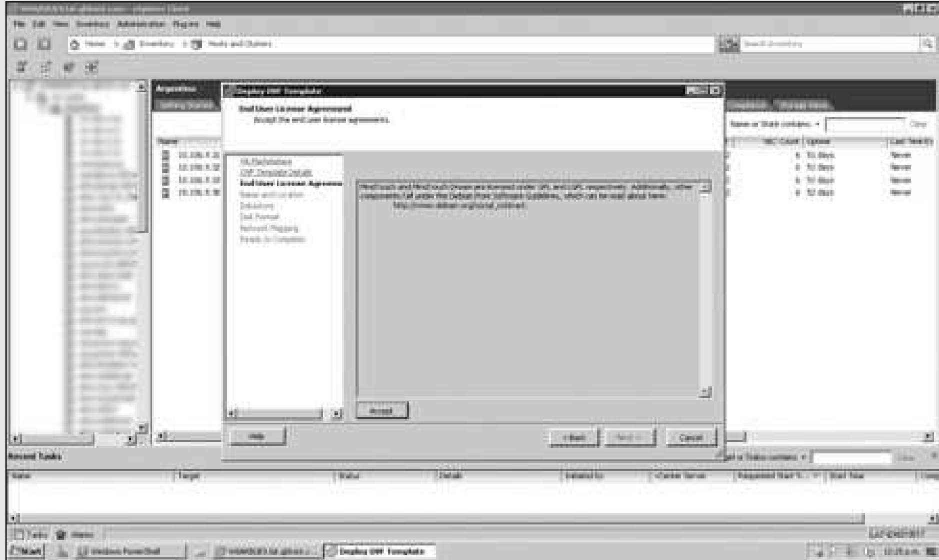


2 Verá una ventana que presenta una serie de alternativas. Para continuar elija, entre todas las posibilidades que se presentan, la aplicación que más le guste o que requiera para implementarla en su organización.

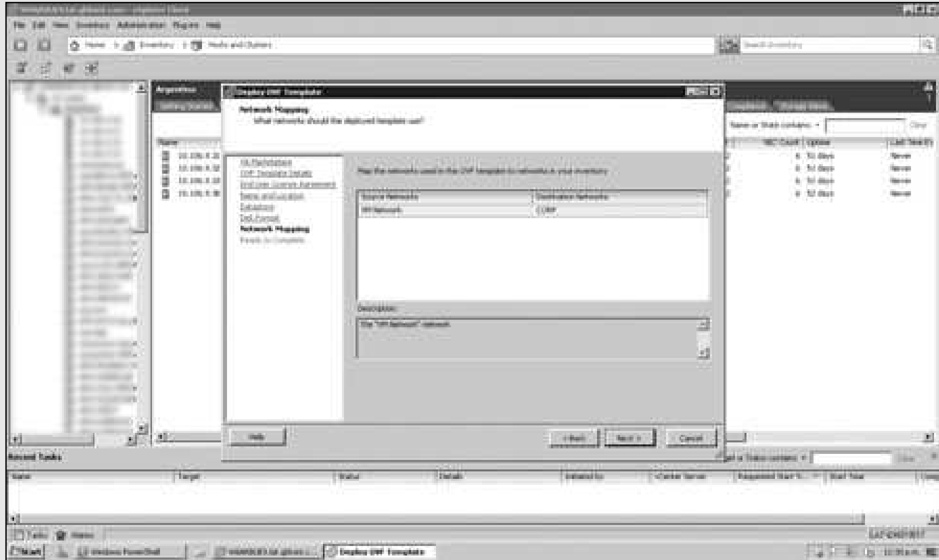


▶

3 Mire la descripción correspondiente a la aplicación que ha seleccionado y luego oprima el botón **Next** para continuar. Acto seguido, acepte el contrato, y presione en forma sucesiva las opciones **Accept** y **Next**.

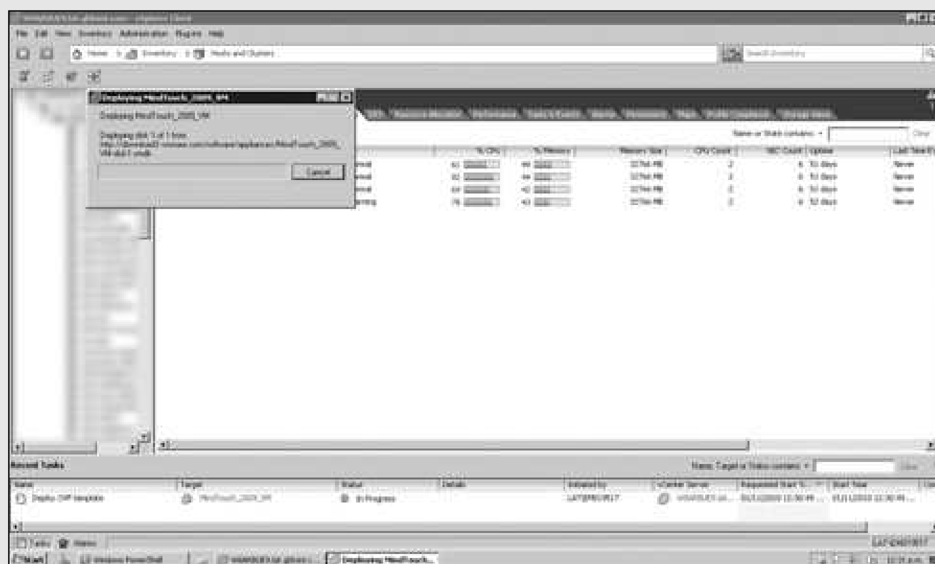


4 En este paso deberá seleccionar el nombre correspondiente, además de los detalles de destino, cluster, unidad de storage y, después, la red que quiere asignarle. Luego de completar todos los datos se presentará un resumen.



▶

▶ 5 Vea el resumen, oprima el botón llamado **Finish**, y así la aplicación abrirá una pantalla donde se detallará el avance de la descarga del servidor virtual.



Una vez finalizada la instalación, estaremos en condiciones de encender el servidor virtual, al igual que cualquier otro. En muchos casos veremos que se prende y queda solamente una consola de administración con la leyenda de que se ha publicado un nuevo servicio web. Debemos acceder a la nueva aplicación desde cualquier navegador. Con **VMware Studio 2.1**, ya podremos crear nuestros propios servidores bajo el formato .OVF, para distribuirlos por toda la empresa. Ésta es una manera de construir aplicaciones virtuales, distribuibles y accesibles rápida y sencillamente. En caso de que queramos borrarla, sólo debemos apagarla, hacer clic derecho en el servidor virtual originado con virtual appliance y elegir **Delete from disk**.

... RESUMEN

En este capítulo vimos muchos temas de virtualización en conjunto con su infraestructura. Nos centramos en las soluciones provistas por VMware, pero hay muchas más que podríamos analizar por nuestra cuenta. Conocimos desde los productos de escritorio, como VMware Player, hasta soluciones para megaempresas, como Virtual Center. Este último es el mejor sistema de todos los nombrados hasta el momento y brinda un altísimo grado de continuidad de negocio; es el mejor en años de desarrollo IT.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 Defina el concepto de virtualización.

2 Describa los detalles de las distintas soluciones de virtualización de VMware.

3 ¿Cuáles son las diferencias entre los servidores ESX y los ESXi?

4 ¿Cuántas formas de administrar un servidor ESX existen? ¿Y uno ESXi?

5 ¿Qué debemos tener en cuenta a la hora de analizar una migración de un servidor SQL?

6 ¿Qué características agrega Virtual Center a la infraestructura virtual?

7 ¿Todos los storage son compatibles con VMware? ¿Dónde podemos consultar la compatibilidad de los equipos?

8 ¿Qué es clonar un servidor y qué diferencias hay con hacer un template?

9 ¿Qué son los virtual appliance?

10 ¿Cuál es la mejor herramienta de virtualización vista hasta el momento?

EJERCICIOS PRÁCTICOS

1 Baje una distribución gratuita de ESXi e instale dos servidores virtuales.

2 Implemente Virtual Center en su empresa. Analice el costo de licencias y de mejoras, y pruébelo.

3 Realice pruebas de storage compartido y cree tres servidores virtuales.

4 Pruebe las capacidades de Vmotion, HA y DRS.

5 Compruebe algunas de las posibilidades de las herramientas de línea de comando que ofrece VMware.

Administrar VMware vSphere

En este capítulo veremos las grandes posibilidades que podremos explotar con vSphere. Conoceremos sus características, y detallaremos cómo instalarlo. Hay algunas herramientas que ya nombramos en el capítulo anterior, pero aquí las detallaremos y aprenderemos a utilizarlas para tener un resguardo de nuestro ambiente virtual.

INTRODUCCIÓN A VSPHERE

VMware vSphere es la mejor solución de virtualización, sin dudas. Viene a completar las herramientas ofrecidas hasta ahora, entre las cuales el último gran recurso era VMware vCenter. VMware vSphere es más completa y cuenta con ciertas características aún mejores. Así, podremos disfrutar de todas las herramientas de vCenter, y aún más. De este modo mejoraremos nuestro objetivo principal: la continuidad del negocio. Veremos los detalles a continuación.

Qué es vSphere y cómo instalarlo

Se trata de un sistema, una consola de administración, muy similar a vCenter, pero más completo. Incluye más características y, por eso, su licencia también es más cara. Se instala sobre un servidor Windows. Trae nuevas funciones que iremos comentando a lo largo de este capítulo, haciendo hincapié en las más importantes.

Figura 1. *Podemos observar la consola de vCenter sin vSphere. Tiene muchas menos opciones, y hay sólo máquinas, hosts y clusters.*

Una de sus funciones nuevas lo destaca en el ambiente de virtualización, y es la posibilidad de tener cero tiempo de bajada para servidores críticos. Hablaremos de esta opción más adelante en este capítulo. Además de esta gran función, incluye otras más con las que ya contábamos en vCenter, como DRS y HA. Entonces, podremos realizar otras acciones que con vCenter no estaban disponibles, como agregar o modificar hardware en caliente. Podremos añadir placas de red, unidades extraíbles,

agrandar discos, agregar memoria, etc. También, a partir de la versión 4, podemos tener configuraciones de **thin provisioning** y placas **vmxnet3**. La consola con la que contamos en vSphere es muy similar a la de vCenter, pero tiene más opciones, se encuentra un poco más organizada y ofrece mayor variedad.

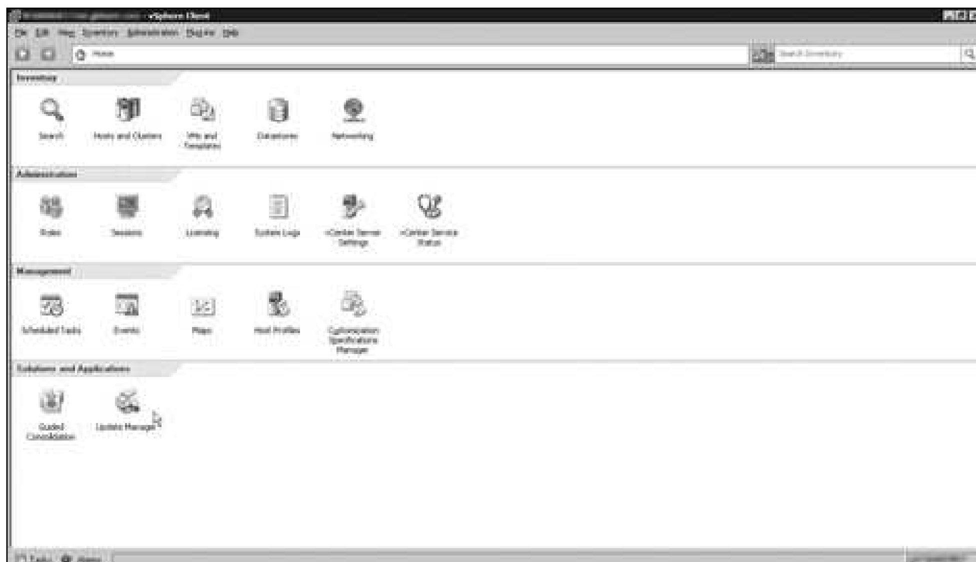


Figura 2. *Podemos observar la consola de vSphere, más precisamente, la vista del home. Encontraremos muchas más opciones que en vCenter.*

Se divide en tres grandes grupos en su **Home**: Inventario, Administración y Gestión. En la parte de Inventario tendremos una vista de **Hosts and Clusters**; otra donde veremos sólo las máquinas virtuales y los templates (plantillas), llamada **VMs and Templates**; otra vista a nivel de **datastores** (unidades de almacenamiento); y una última de switches virtuales y red llamada **Networking**. En la vista de Administración es posible configurar los roles de los distintos usuarios, controlar las sesiones, ver los datos de las licencias, chequear logs, configurar ciertas opciones de vCenter, ver el estado de los servicios y obtener un reporte de licencias. Por último, en la parte de Gestión podemos configurar tareas programadas,

HOSTS Y CLUSTER

Debemos saber que se llama hosts a los nodos ESX/ESXi con los que contamos en nuestra infraestructura virtual. Estos hosts pueden ser agrupados en distintos conjuntos de carga balanceada y tolerante a fallos. A estos grupos se los conoce como cluster. Es posible tener uno o más clusters administrados con el sistema denominado vSphere.

ver los eventos y los mapas de conexiones, administrar los perfiles de usuarios, y un par de opciones más. También, si se instala algún tipo de plugin, lo veremos en la zona inferior del menú principal, en **Solutions and Applications**.
Para la instalación, existen ciertos requisitos que nos obligan a modernizar la infraestructura. En principio, se puede instalar sólo en arquitectura de 64 bits. Soporta varios microprocesadores, pero también en este punto estamos un poco limitados. Los procesadores que se mencionan en la guía de instalación son AMD Opteron, Intel Xeon con varios modelos e Intel Nehalem. En cuanto a memoria RAM, se precisan 2 GB como mínimo, al igual que para la instalación de cualquier ESX/ESXi. También necesitamos alguno de estos adaptadores de red genéricos: Broadcom NetXtreme, de Gigabit, o Intel PRO 1000. Hay una serie de controladores de placas de fibra soportados y de storage soportados. Recordemos que es posible chequear toda la compatibilidad haciendo una consulta de nuestro hardware en la página siguiente: **www.vmware.com/resources/compatibility**.
Durante el proceso de instalación, el asistente nos pide una base de datos y también tenemos la posibilidad de instalar MsSQL Express para crearla. Serán dos bases de datos las que precisemos: una para el manejo de transacciones de vSphere y otra para manejar las actualizaciones. Al igual que con vCenter, podemos instalar estas bases de datos en el mismo equipo o en uno separado. Debemos tener en cuenta que, a medida que nuestra infraestructura virtual vaya creciendo, las bases de datos también lo harán. Dependiendo de si queremos una infraestructura chica o una inmensa, instalaremos las bases de datos en el mismo servidor o en otro separado. Todo el proceso para hacerlo es sencillo, y no hay demasiadas complicaciones si cumplimos con los requisitos de hardware y software. A continuación, veremos paso a paso cómo instalar vSphere en la empresa para comenzar a optimizar nuestro objetivo principal.

Instalar vSphere — PASO A PASO

1 Coloque la unidad de disco en el futuro servidor de vSphere. Entre en el menú principal y haga clic en vCenter Server. Luego oprima **Next** tres veces. Se le dará la bienvenida, y se mostrará la información de la patente y el contrato de licencia.



▶

▶

2 Ingrese su nombre, el de su organización y una llave de licencia. Si no la posee, se activará el modo evaluación. Oprima **Next**.



3 Elija instalar MsSQL Express 2005 o usar algún otro tipo de base de datos. Para este último punto, deberá tener un DSN creado.



4 Ingrese un nombre de usuario o utilice la cuenta del sistema para loguearse en MsSQL. Con este usuario, MsSQL se instalará como servicio en el equipo; esto quiere decir que el usuario debe tener privilegios de administrador en él.



▶

▶

5 Para continuar, será necesario que seleccione una ubicación para la carpeta de instalación de VMware vSphere. Luego, haga clic en **Next** y elija la primera opción para crear un servidor vCenter independiente.



6 Cambie los puertos de conexión según las reglas de firewalls y de redes de la compañía. Recuérdelos para poder conectarse luego.



7 Elija el tamaño que tendrá su granja de servidores: Small, Medium o Large. Oprima **Next** y luego **Install**. Espere hasta que la instalación termine.



vSphere como centro de licenciamiento

Al instalar vSphere, se instala en forma automática el plugin de servidor de licencias. Desde la consola de vSphere podremos administrar más fácilmente todas las llaves, ver cuántos servidores están utilizando cada una y cuántas nos falta usar según el contrato. Esto quiere decir que si tenemos nuestros ESXs con una licencia propia, una llave configurada en cada uno, podremos colocar estas llaves en el servidor de licencia y configurar el servidor vSphere en los ESXs.

El plugin para administrar las licencias se instala por defecto en la última versión al publicar este libro, la 4.1; no sucede así en versiones anteriores, en donde había que instalarlo en forma manual. Al activarse el plugin, podemos entrar en la consola desde el menú **Home/Administration/Licensing**.

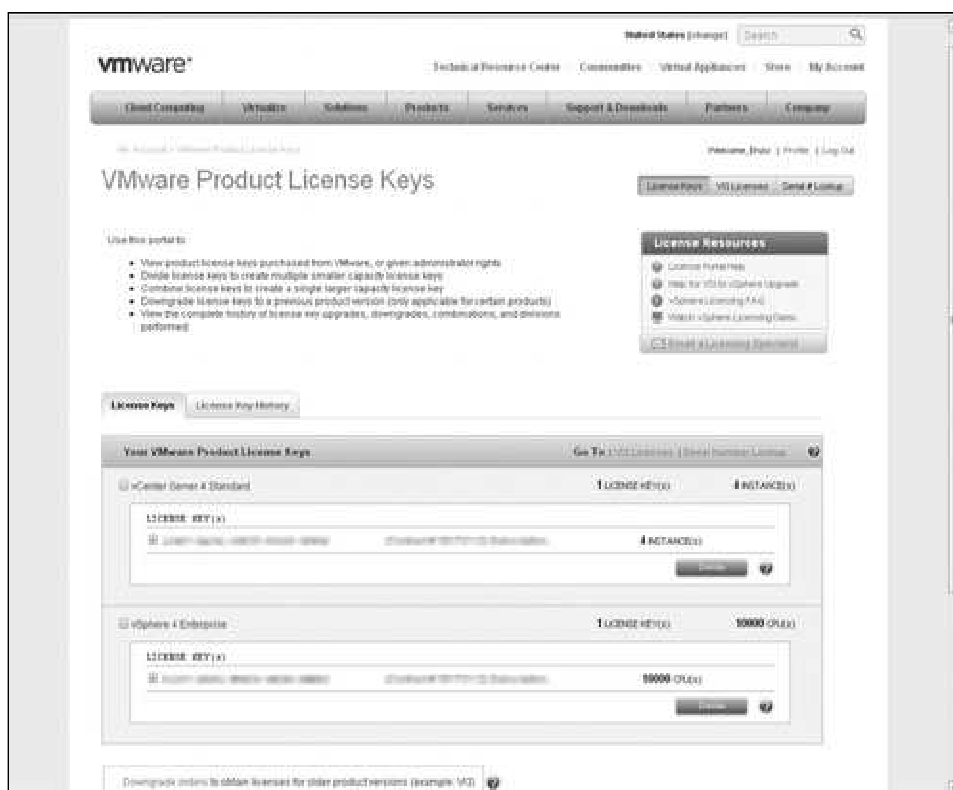


***Figura 3.** Vemos el sitio de licencias una vez que entramos en el portal de VMware con nuestras credenciales. Podemos observar un resumen de las licencias y nuestros productos.*

Hay un plugin que también se instala con vSphere, llamado **Licensing Reporting Manager**, que nos deja sacar reportes sobre nuestros usos de licencias en la infraestructura virtual. Si no lo vemos en la **home** de la consola (menú principal), debemos ir al menú **Plug-ins** y allí elegir **Manage Plug-ins**. Allí veremos un listado con

todos los plugins habilitados en vSphere; buscamos el de **Licensing Reporting Manager**, hacemos clic derecho y seleccionamos **Enable**. Para habilitar cualquier plugin que veamos deshabilitado, realizamos la misma operación.

Cómo hacer un cluster

Es importante que tengamos en cuenta que los clusters se encargan de agrupar a los nodos ESX/ESXi para balancear las cargas de las demandas de CPU y memoria de la computadora. Obviamente, todos los nodos que configuremos en el mismo cluster deben poder acceder a la misma unidad de storage. Cada LUN que tengamos se configura en cada ESX/ESXi.

Todos los nodos que conforman el cluster deben tener las mismas características de CPU e idénticas configuraciones de red. De la misma forma es importante que cuenten con los mismos switches virtuales creados con los mismos nombres. Todos estos requisitos son para que los servidores virtuales puedan ir de un nodo a otro sin interferencias de ningún tipo. Debemos saber que la realización de este movimiento se efectúa en forma completamente automática, mediante la configuración de **DRS** que debemos tener habilitada en nuestro cluster. Veremos más adelante otros detalles sobre DRS.

Al crear un cluster, también se debe activar la opción **HA**, que permite que nuestros equipos sean reiniciados y movidos de nodo si aquél en el que se alojan en ese momento falla. Esto nos permite tener siempre funcionando nuestra infraestructura virtual si los servicios que hay en los servidores se levantan automáticamente. Si tenemos **DPM** habilitado, podremos apagar y encender nodos ESX que no estén siendo utilizados, dependiendo de la demanda. También, mientras configuramos el cluster, podremos elegir entre activar o no una mayor compatibilidad para Vmotion entre los nodos ESX que lo conforman. Esta opción se llama **EVC** (*Enhanced VMotion Compatibility*).

Es importante saber que es posible realizar la definición de un cluster para microprocesadores AMD o Intel; de esta forma podremos utilizar las nuevas opciones a nivel de hardware de microprocesadores Flex Migration para Intel, y AMD-V Extended Migration Technologies para AMD.



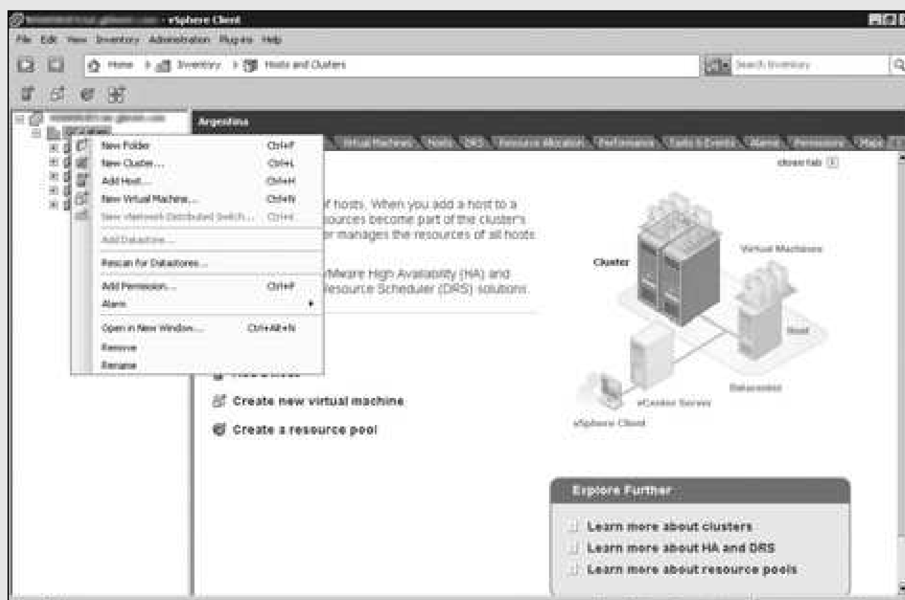
FALLAS EN EL SERVIDOR DE LICENCIAS

El servidor de licencias puede fallar y esto dejará sin licencias a todos los nodos ESX/ESXi. VMware nos da la posibilidad de tenerlo caído durante 14 días, al igual que en vCenter, hasta repararlo. Esto mantiene las licencias en los nodos durante ese tiempo y, luego, los nodos pasan a estar en modo evaluación o con sus licencias previas.

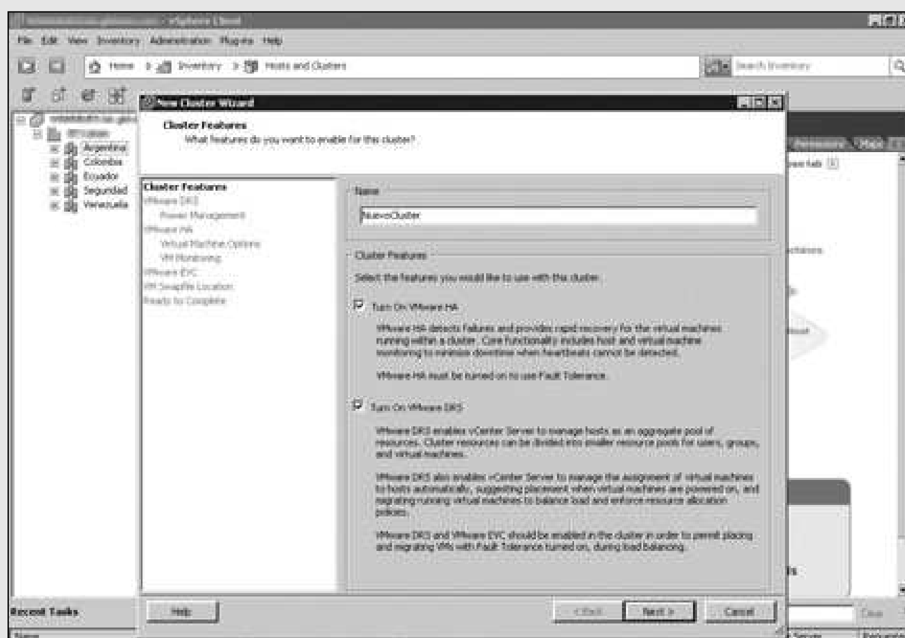
■ Armar un cluster en vSphere

PASO A PASO

1 Abra la consola de vSphere y haga clic derecho en el cluster. Elija **New Cluster...**

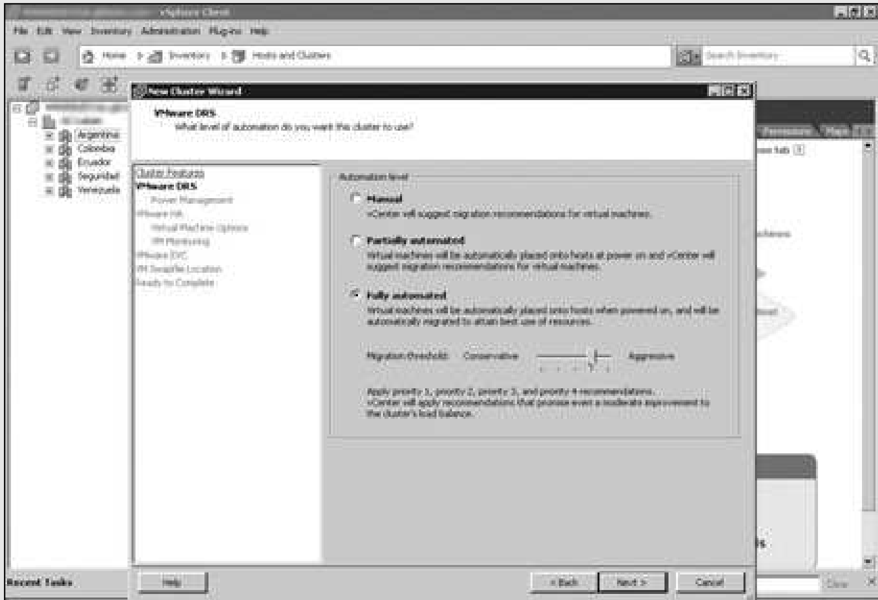


2 Coloque un nombre y seleccione las opciones de **HA** y **DRS** para habilitarlas.

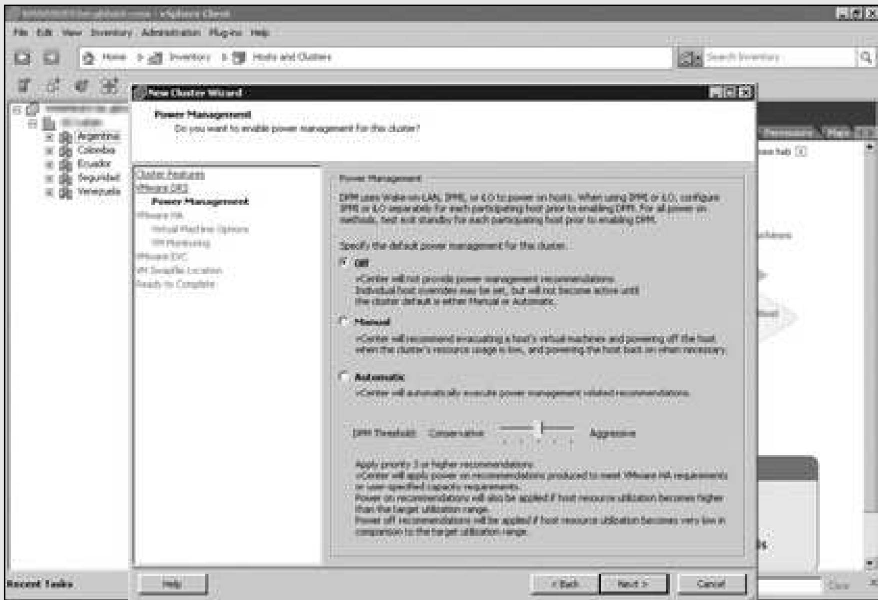


▶

3 Elija las opciones de DRS: **Manual** o **Partially automated** para que no se muevan automáticamente. Marque **Fully automated** para modo automático. Elija un modo de agresividad medio.

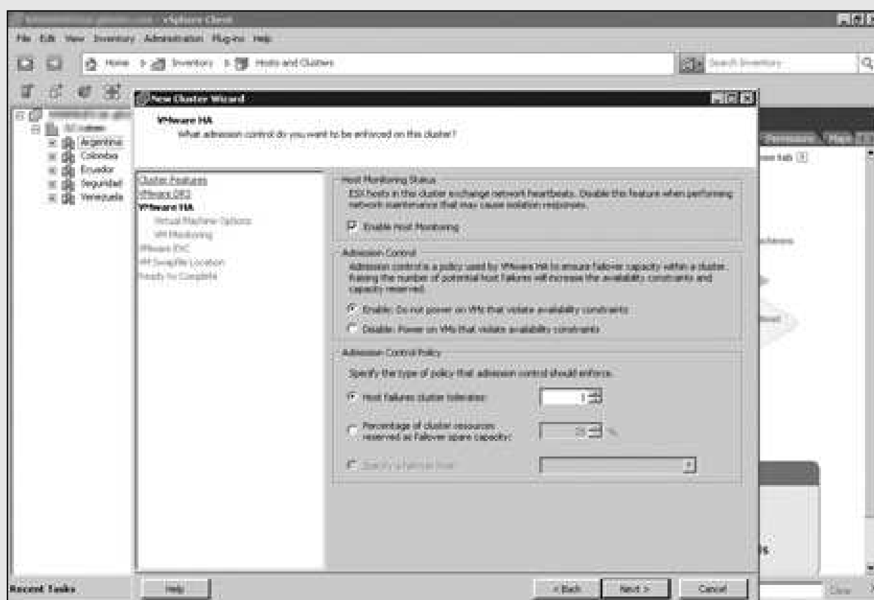


4 Seleccione las opciones de DPM; para este ejemplo, déjelo desactivado eligiendo **Off**.

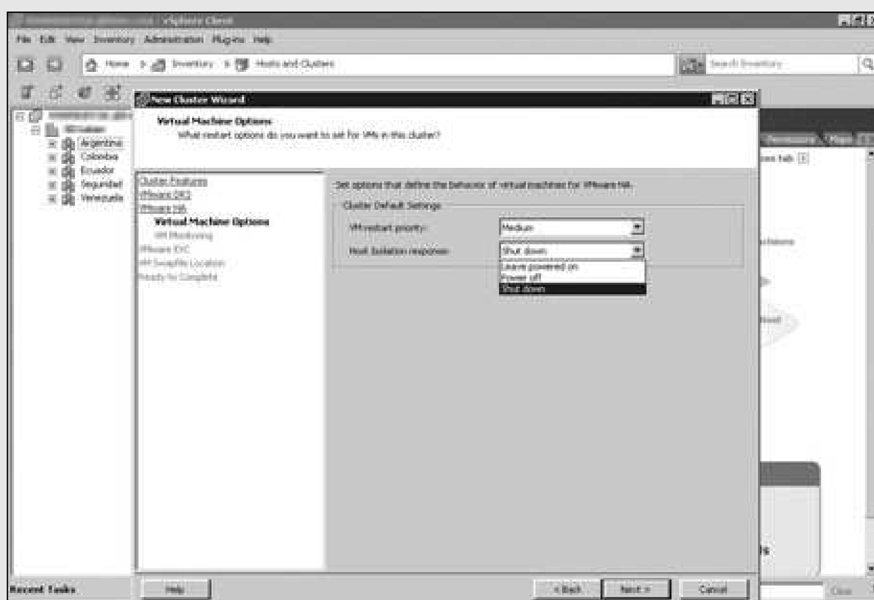


▶

5 Haga clic en **Enable Host Monitoring**. Luego habilite la opción **Enable** en **Admission Control** y elija una regla de **failover** en **Admission Control Policy**.

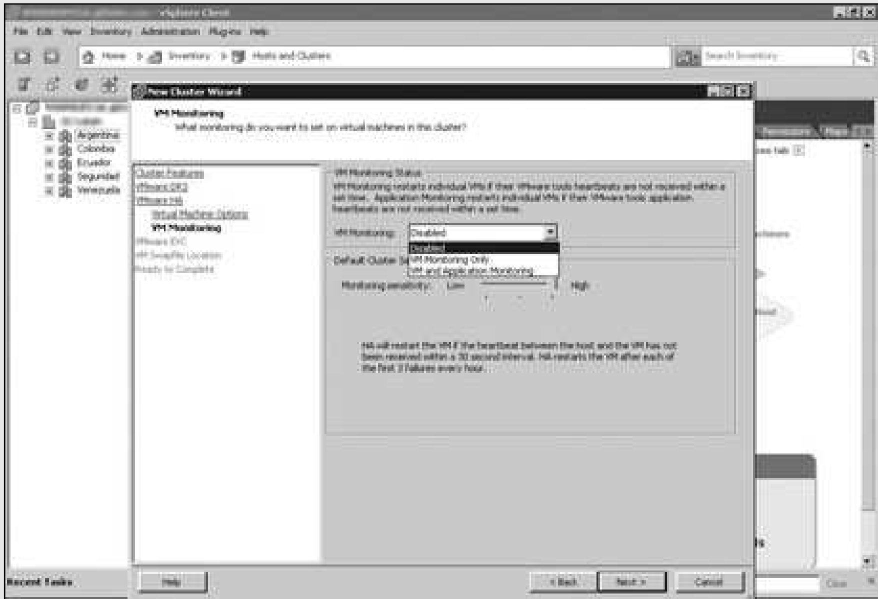


6 Ahora escoja una política para la alta disponibilidad; las máquinas de nivel bajo, medio o alto se apagarán si así sucediera.

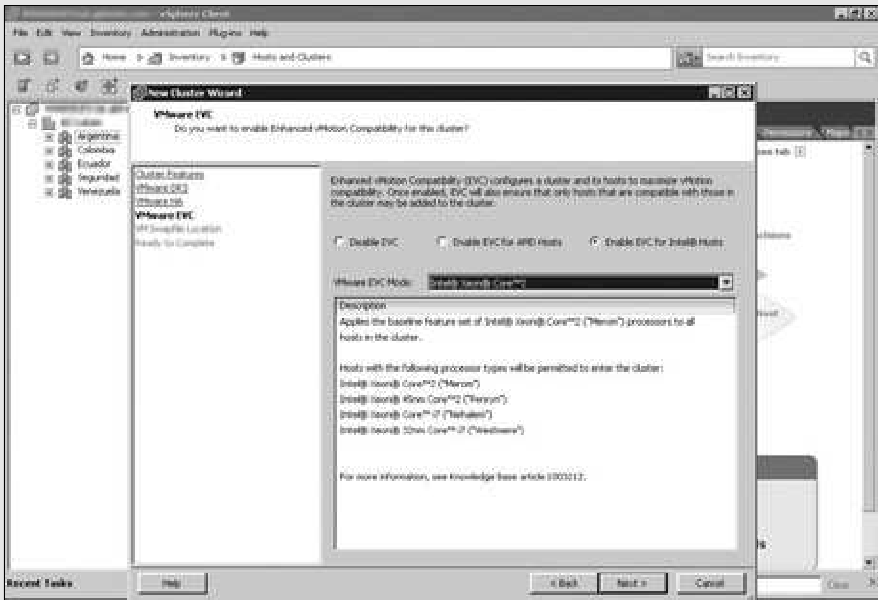


▶

7 Establezca una política para monitorear los servidores virtuales y los appliances. Esta opción reiniciará el sistema si descubre una falla.

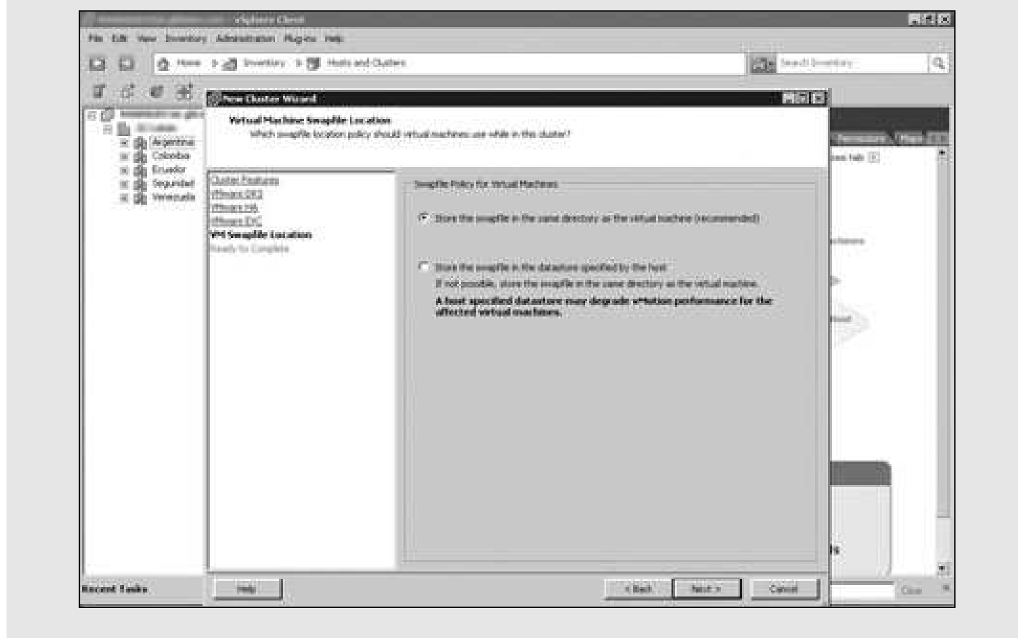


8 Puede habilitar la compatibilidad con algún modelo de microprocesador en especial o déjelo deshabilitado eligiendo **Disable EVC**.



▶

▶ **9** Luego escoja dónde almacenar los archivos swap; deje la primera opción, que es la recomendada. Presione **Next**, luego vea el resumen y pulse el botón **Finish**.



Cómo agregar nodos ESX

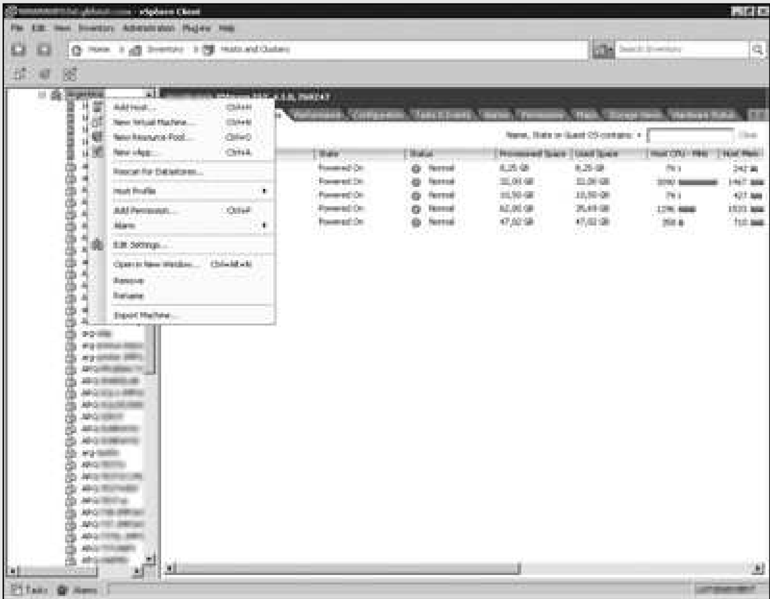
Luego de crear nuestro cluster, veremos ahora cómo anexarle nodos ESX o ESXi. Debemos tener en cuenta que ésta es una tarea muy fácil y es la forma de que los nodos ESX/ESXi sean administrados con el sistema denominado vSphere. Puede haber ciertos errores si tenemos el firewall del nodo habilitado, pero generalmente, no hay problemas mayores. Los nodos que agreguemos a un cluster deben ser iguales. En cualquier caso, si no estamos seguros, el sistema vSphere se encargará de alertarnos en forma inmediata acerca de que el nodo ESX por agregar no es compatible con los actuales nodos que corresponden al cluster.

DNS (DOMAIN NAME SYSTEM)

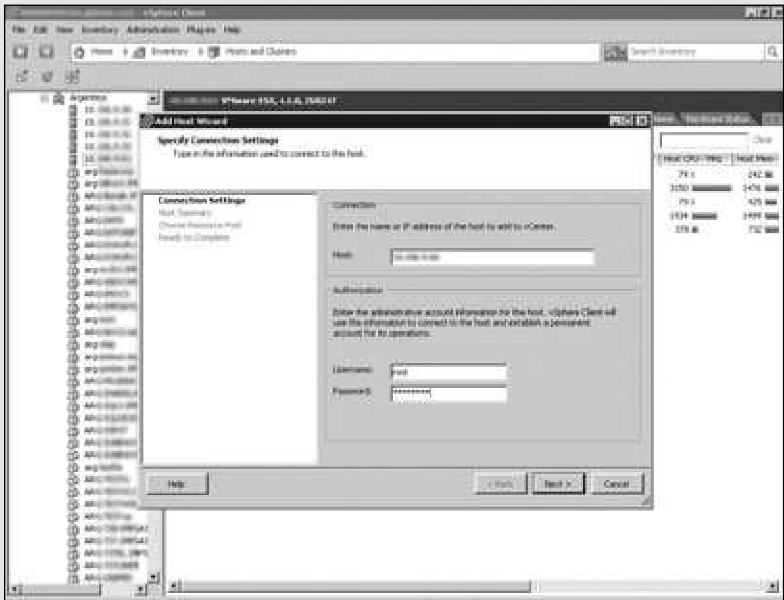
Es un sistema de nomenclaturas jerárquico, que puede administrar computadoras, servicios o cualquier elemento conectado a la red. Su función más importante es traducir nombre inteligibles para los humanos en identificadores binarios asociados con los equipos en la red. Así, es posible localizar y redireccionar todos y cada uno de los elementos.

■ Agregar nodos ESX — PASO A PASO

1 Abra la consola de vSphere y haga clic derecho en el cluster. Elija la opción **Add host**.



2 Coloque los datos de la dirección IP del servidor ESX/ESXi y también los datos del usuario **root** para conectarse.



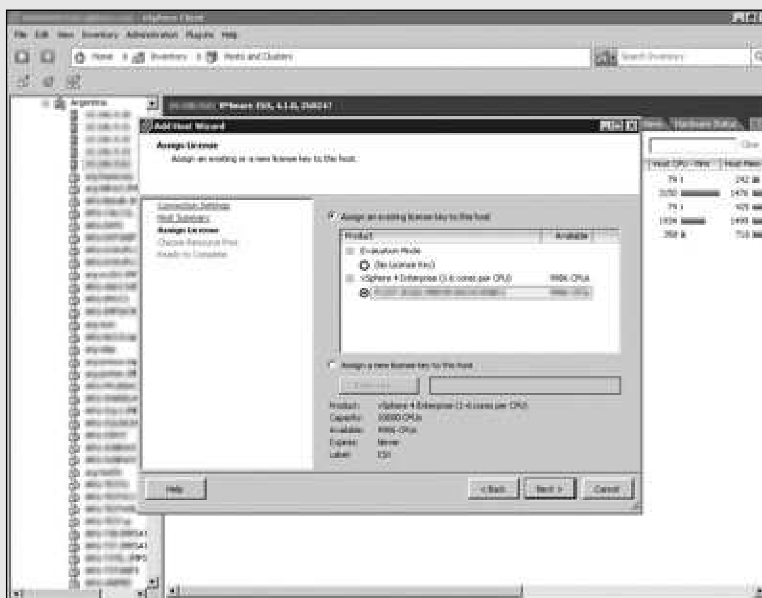


▶

3 En el cartel donde aparece una advertencia haga clic en **Yes**; sólo se da información sobre un certificado SHA1 para el nodo ESX/ESXi.



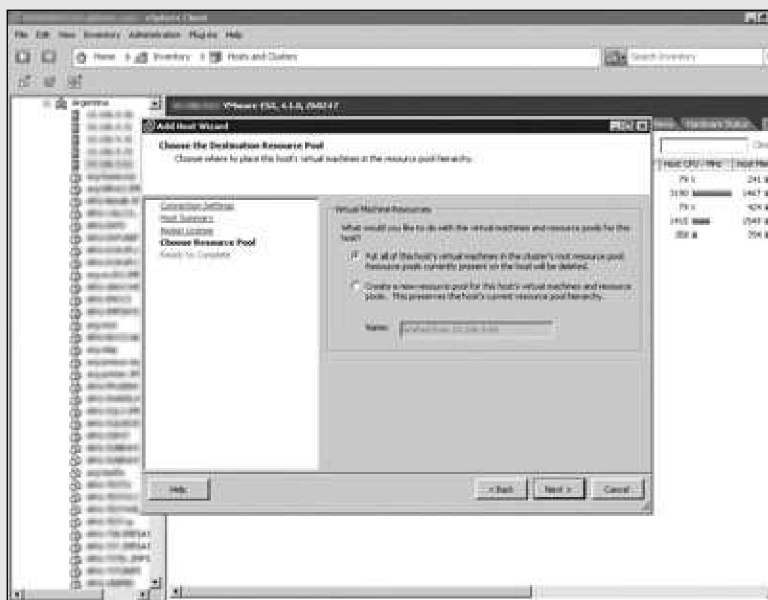
4 Elija una llave de licencia para el nodo ESX/ESXi; puede elegir uno ya cargado en vSphere, dejarlo en modo evaluación o ingresar algún otro.



▶

▶

5 Configure cómo administrar los recursos del nodo por conectar; deje la primera opción para poner todo en un mismo gran pool de recursos. Oprima **Next**, mire el resumen y presione **Finish**.



En caso de que queramos chequear la funcionalidad de un nodo antes de ponerlo en la granja en modo automático, nos conviene desactivar DRS antes de anexar el nuevo nodo. Entonces, una vez deshabilitado, incorporamos el nuevo nodo y hacemos una prueba manual con vMotion para verificar si el servidor virtual no tiene interrupciones, si no se corrompe al pasar o si ocurre algo inesperado. Luego de hacer varias pruebas de ida y de vuelta, configuramos DRS otra vez para todo el cluster de manera automática. Es recomendable realizar también esta práctica cuando necesitamos sacar un nodo del cluster. La idea es desactivar el DRS automático y mover uno a uno los servidores virtuales hacia los otros nodos, verificando las cargas con vMotion. Una vez que el nodo que queremos retirar está sin máquinas virtuales, procedemos a apagarlo, actualizarlo o lo que queramos hacer. Hay una opción automática que realiza estas acciones de mover los servidores a otro lugar para desactivar el nodo. Sólo tenemos que hacer clic derecho y elegir **Enter Maintenance Mode**. Esto moverá los servidores virtuales y distinguirá el nodo en nuestro cluster como en modo mantenimiento. Si todavía tenemos activado DRS, sólo se desactivará este nodo en cuestión, y el DRS se seguirá usando en los otros; no perderemos la carga balanceada, pero resultará un tanto peligroso. Lo importante es poder elegir cómo hacerlo.

HERRAMIENTAS DE VSPHERE

Es necesario tener en cuenta que con el sistema VMware vSphere se incluyen varias herramientas, las cuales se encargarán de facilitar el proceso de administración de los servidores y darán a la empresa la máxima capacidad de continuidad de negocio posible en estos tiempos. Muchas de ellas ya pueden utilizarse instalando vCenter, pero explicaremos los detalles a continuación. Entre las opciones existentes, encontramos las conocidas como **Vmotion** y **Storage Vmotion**, **HA** (*High Availability*), **DRS** (*Distributed Resource Scheluder*), **Fault Tolerance** y **Update Manager**.

Qué es Vmotion

Empecemos a analizar las herramientas que nos ofrece vSphere, comenzando, nada más y nada menos, que con Vmotion. Se trata de una herramienta esencial en la infraestructura virtual. Básicamente, nos permite realizar el movimiento de un servidor virtual de un nodo ESX/ESXi a otro nodo. Debemos saber que esta opción es realmente fantástica, porque no tendremos ninguna pérdida de conexión ni de bajada de servicio al mover el equipo. Es más, podremos darnos cuenta de que las pruebas que se realizan en las presentaciones del producto muestran un video en funcionamiento al momento de hacerle Vmotion al servidor, y en verdad no se distingue ninguna pérdida en la imagen presentada. Esto se debe al sistema de archivos que utilizan los ESX/ESXi, denominado **VMFS**.

Los datos de los servidores virtuales están físicamente en la LUN del storage; sólo se comparten entre los nodos los recursos de CPU y memoria. Entonces, al mover un servidor virtual, la tarea se realiza rápidamente porque, en realidad, hay pocas cosas por mover para que quede funcionando en otro nodo. El estado de la memoria activa y en ejecución se pasa rápidamente hacia el otro nodo por una red de alta velocidad. Es por eso que la conexión de red debería ser a **Gbit** (utilizando un switch que soporte Gbit y cables de categoría 6). Para habilitar esta característica en vSphere, debemos tener una tarjeta de red dedicada en cada nodo ESX/ESXi con una VLAN propia entre todas ellas. Sin esta VLAN configurada, Vmotion no puede funcionar correctamente.



SISTEMA DE ARCHIVOS VMFS

Es un sistema de archivos para clusters, exclusivo de VMware, que da privilegio a los nodos ESX/ESXi para que puedan leer y escribir de manera coordinada y simultánea los mismos archivos al mismo tiempo en particiones SCSi. Es posible conectar hasta 32 nodos al mismo volumen VMFS, que puede tener un tamaño máximo de 2 TB.

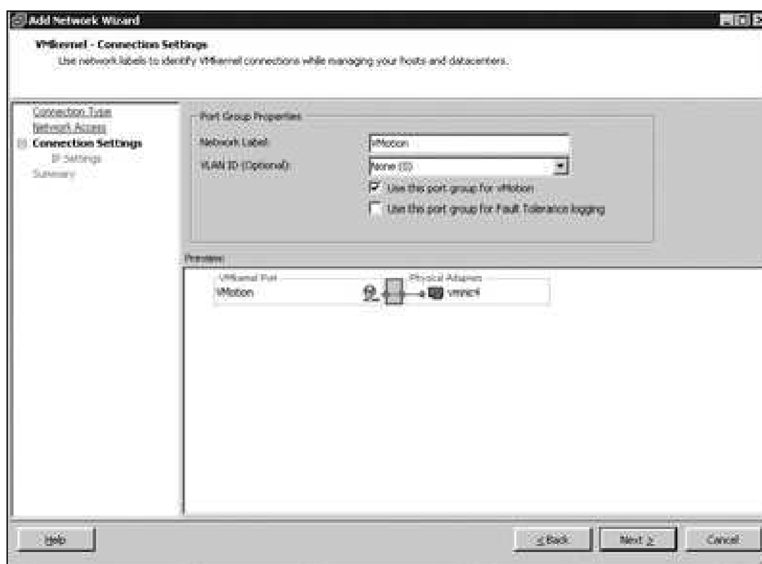


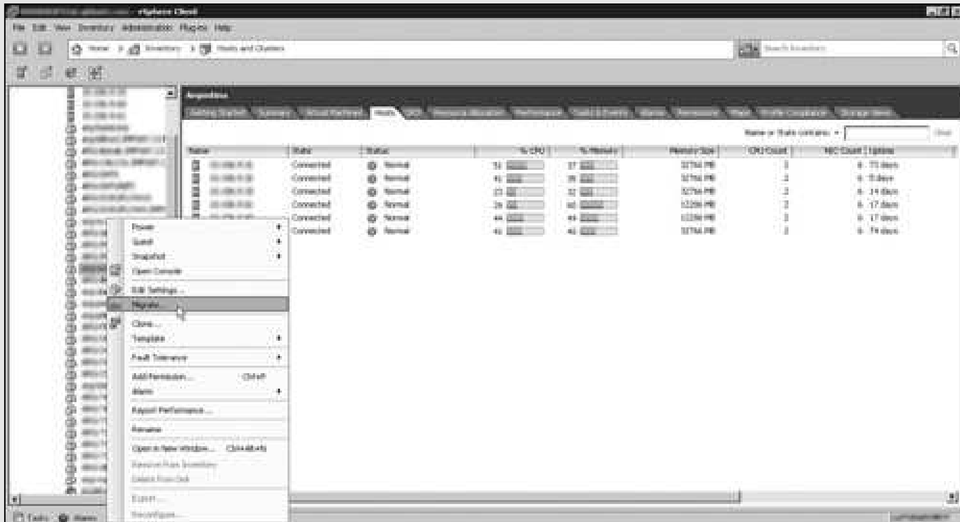
***Figura 4.** Al momento de crear un nuevo switch virtual, es muy importante seleccionar el tipo VMkernel y marcar la casilla para que vSphere sepa que esa placa será usada para Vmotion.*

Una vez que hayamos realizado la configuración correspondiente a la red para Vmotion, será necesario que efectuemos una prueba de migración. Las migraciones pueden realizarse en caliente o en frío. Esto quiere decir que se pueden hacer teniendo el servidor encendido o apagado. Vmotion es indispensable para crear centros de cómputos dinámicos y automatizados. Así, es posible realizar las tareas de mantenimiento del hardware físico sin afectar la continuidad del negocio en ningún aspecto. Es una tecnología que corresponde al año 2004, es decir que, al momento de escribir este libro, tiene un desarrollo de más de seis años. Para conectar los nodos al storage y utilizar Vmotion, además de poder conectar una **SAN** (*Storage Area Network*) por fibra, también soporta compatibilidad con **NAS** (*Network Attached Storage*) y **SAN iSCSI**, los cuales son sistemas de almacenamiento mucho más económicos y accesibles que otras alternativas.
Las tareas de migración también poseen prioridades y pueden programarse para que sean realizadas a determinada hora del día. Podríamos tener un problema si un servidor virtual se moviera cuando no se tiene que mover por alguna razón. Supongamos que estamos realizando una tarea de configuración de una placa de red en un nodo, y algún administrador pone en Vmotion un servidor virtual con destino al nodo que estamos arreglando. En ese caso, podría perderse el servicio y, por lo tanto, la continuidad del negocio. Para esto, la consola tiene debajo una vista de todas las tareas que se realizan en vSphere, dentro de la solapa **Tasks**. Ante cualquier circunstancia parecida, podemos cancelar la operación. También la comunicación en este caso se presenta como una tarea esencial.

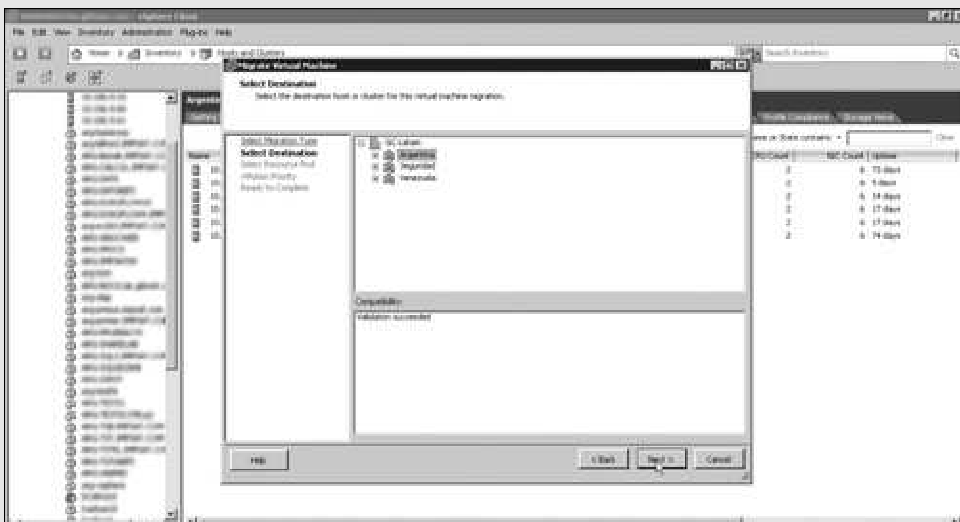
Hacer Vmotion a un servidor

PASO A PASO

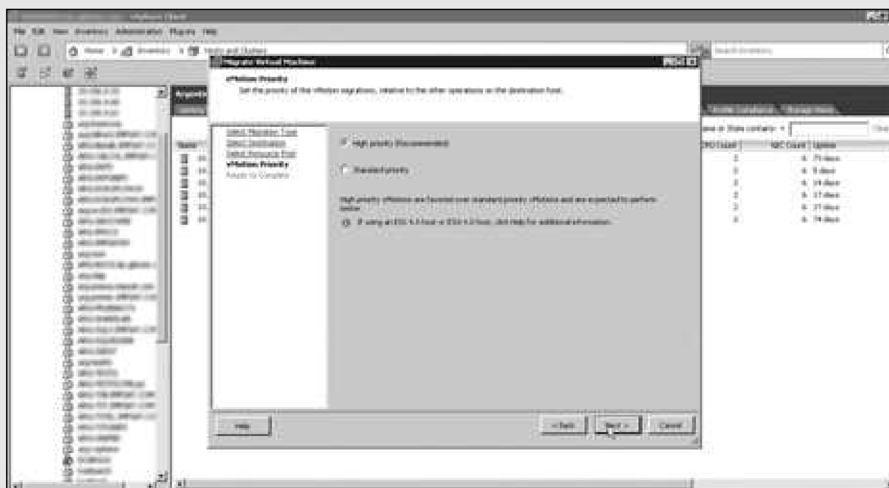
1 Abra la consola de vSphere y sitúese sobre el servidor virtual que pretende mover a otro host. Tenga en cuenta la solapa **Summary**, que le indica en qué host se encuentra. Haga clic derecho y elija **Migrate...**



2 Para continuar, deberá elegir la primera opción de **Change host**; oprima el botón denominado **Next** y posteriormente seleccione el cluster a donde ubicará el servidor virtual. Si elige el cluster DRS, elegirá dónde ubicarlo; si no, puede elegir directamente un host expandiendo el árbol.



3 Seleccione el pool de recursos que va a consumir el servidor virtual y luego presione **Next**. A continuación, elija la prioridad con la que realizará la tarea. Oprima **Next**, vea el resumen y comience a migrar. Aparecerá el detalle en la solapa **Tasks**, en la parte inferior de la consola.



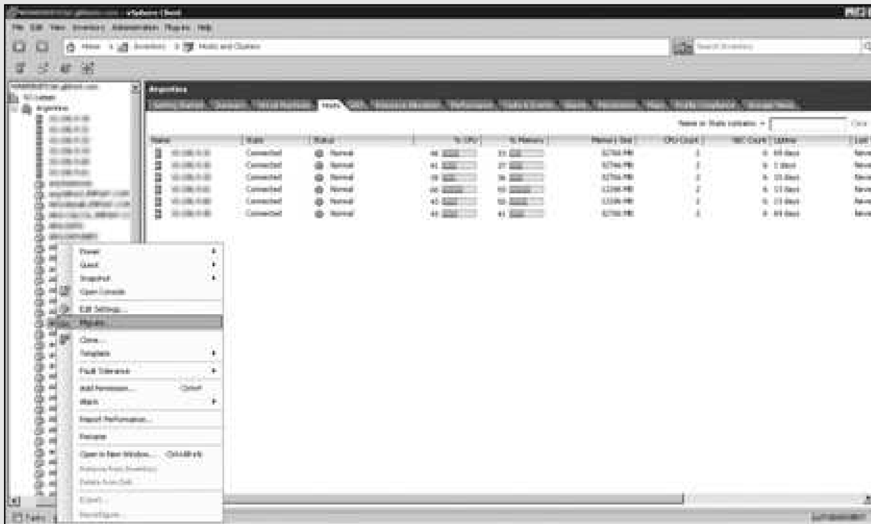
Qué es Storage Vmotion

Storage Vmotion es, simplemente, la misma filosofía que Vmotion, pero en este caso se corre la máquina de ubicación física, no de nodo. Tampoco hay pérdida de datos ni de comunicación. También existe la **migración en frío** y la **migración en caliente** sin ningún tipo de bajada de servicios. Esto nos permitiría deshacernos de storage antiguos y difíciles de gestionar; y aceleraríamos en gran medida las migraciones con respecto a los sistemas tradicionales, sin interrupciones y sin coordinar la bajada de servicios, porque no existirían. Storage Vmotion copia el directorio principal a la nueva ubicación antes de mover el archivo de disco del servidor virtual (**archivo vmdk**). Este directorio tiene los archivos de configuración, intercambio y registros del servidor virtual. Luego, copia el contenido de todo el archivo vmdk en el destino y utiliza el seguimiento de los bloques modificados manteniendo la integridad de los datos en el proceso de migración. Verifica las zonas del disco que se han escrito en el primer contacto entre la **fuente** - **destino** y realiza una segunda **iteración** de la copia de las zonas que cambiaron desde la primera iteración, y así sucesivamente, hasta que no haya más cambios. Luego, el servidor virtual es suspendido y vuelto a despertar rápidamente; allí empiezan a utilizarse el directorio principal y los archivos de la ubicación destino. Antes de que el servidor esté completamente operativo, Storage Vmotion borra los archivos en la fuente para

asegurar la integridad de la información. Como ya hemos visto en el capítulo anterior, existen dos opciones para manejar la información en disco: una ligera y otra pesada; que en inglés se conocen como **thin configuration** (*thin provisioning*) y **thick configuration**, respectivamente. La primera es la más recomendable, ya que da al servidor virtual sólo el espacio en disco realmente utilizado. Existe un problema si todos los servers con thin configuration comienzan rápidamente a crecer. Entonces, hacer un mix sería lo mejor para aprovechar al máximo nuestro espacio en el storage. Esta configuración se decide a la hora de crear el servidor virtual, y no hay vuelta atrás, **sólo migrando el equipo con Storage Vmotion podemos realizar el cambio**. Esto es importante si tenemos muchos servidores creados en thick configuration desaprovechando el disco físico.

Hacer un Storage Vmotion — PASO A PASO

1 Abra la consola vSphere y haga clic derecho en un servidor virtual; elija **Migrate** para empezar la tarea.



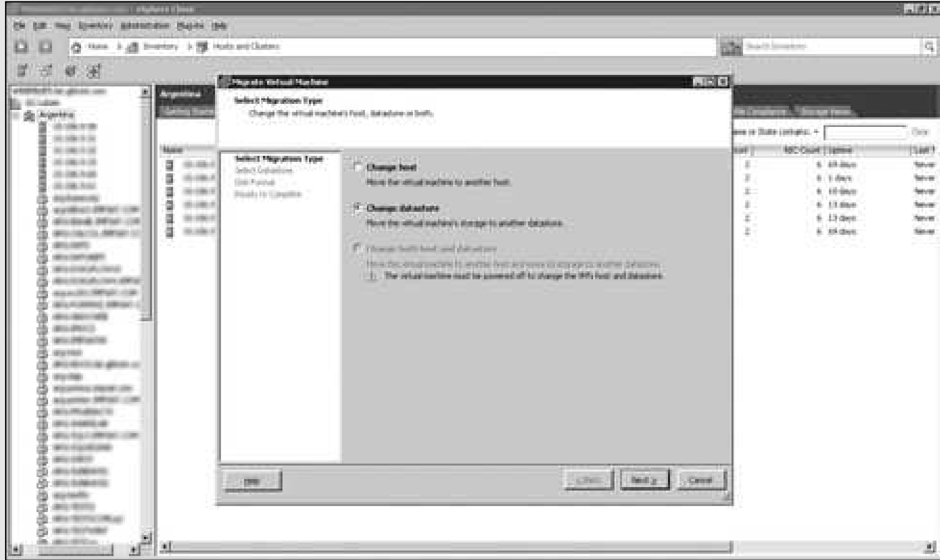
►

SERVIDOR EN SPARE

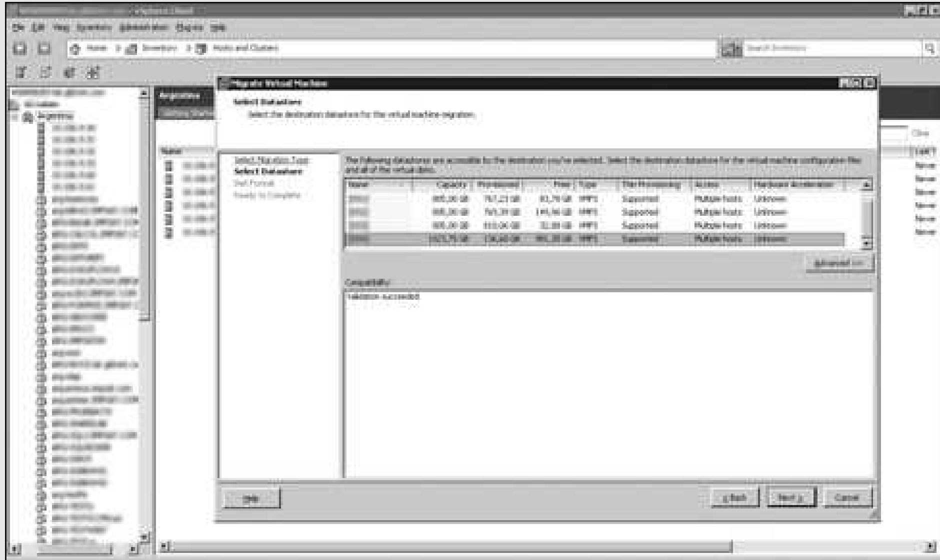
Tener un equipo en spare significa tener un equipo igual que estará esperando apagado hasta que el otro se rompa. Entonces, ante la aparición de un fallo de hardware, el cual podría ser de disco, de memoria, de CPU o de placa madre, nos permitiría hacer un cambio rápido de los elementos que lo conforman y volver a tenerlo online.

▶

2 Para continuar, en la ventana que se presenta deberá elegir la segunda opción, denominada **Change datastore**; de esta forma podrá realizar la migración del servidor virtual a un storage diferente.

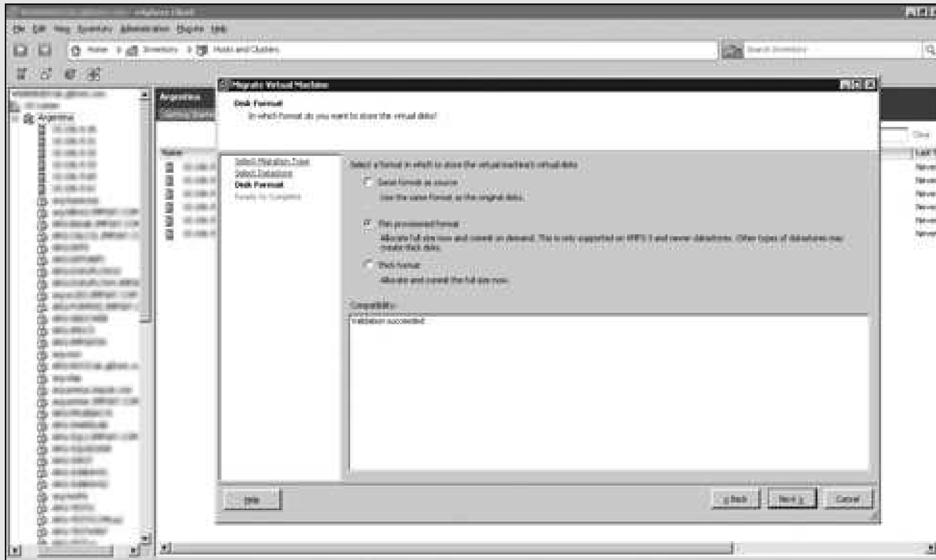


3 Luego, será necesario que seleccione el storage al cual moverá el servidor virtual, para lo cual se presentará un listado con las opciones disponibles; tenga en cuenta el espacio libre que necesita el servidor.



▶

► 4 En este paso elija el formato de disco. Recuerde escoger la opción denominada **Thick format** para equipos que tendrán sus discos estáticos, y **thin provisioning** para aquellos con discos de crecimiento dinámico. Oprima **Next**, observe el resumen y presione sobre el botón llamado **Finish** para terminar.



Descripción de HA

HA nos permite tener alta disponibilidad de nuestros equipos virtuales, algo inimaginable con servidores físicos. Antes, si un servidor físico fallaba, el servicio moría con él hasta que lo arreglábamos. Se utilizaban varios métodos de recuperación, backups, imágenes de recuperación o un equipo en **spare**.
Las soluciones anteriores implican una gran inversión de dinero si necesitamos un spare por cada modelo de servidor que tengamos. Si nuestra empresa abarca varias localidades, ciudades o países, deberíamos tener uno en cada lugar para hacer un cambio rápido y obtener el mínimo tiempo de bajada del servicio posible. Con el advenimiento de la virtualización, el hardware pasa a ser un objeto virtual y mucho más maleable que el físico. Con HA activado en nuestra infraestructura virtual, si un nodo ESX falla por alguna cuestión de hardware, error de energía o cualquier otra causa, todos los servidores virtuales son movidos hacia otro nodo que tenga recursos disponibles y son reiniciados automáticamente. Esto marca una gran diferencia en nuestros números mensuales. Las cifras suben estrepitosamente, dándonos un 97% a 100% de disponibilidad. Si el sistema operativo provoca un error, el servicio de HA puede detectarlo y reiniciar la máquina.

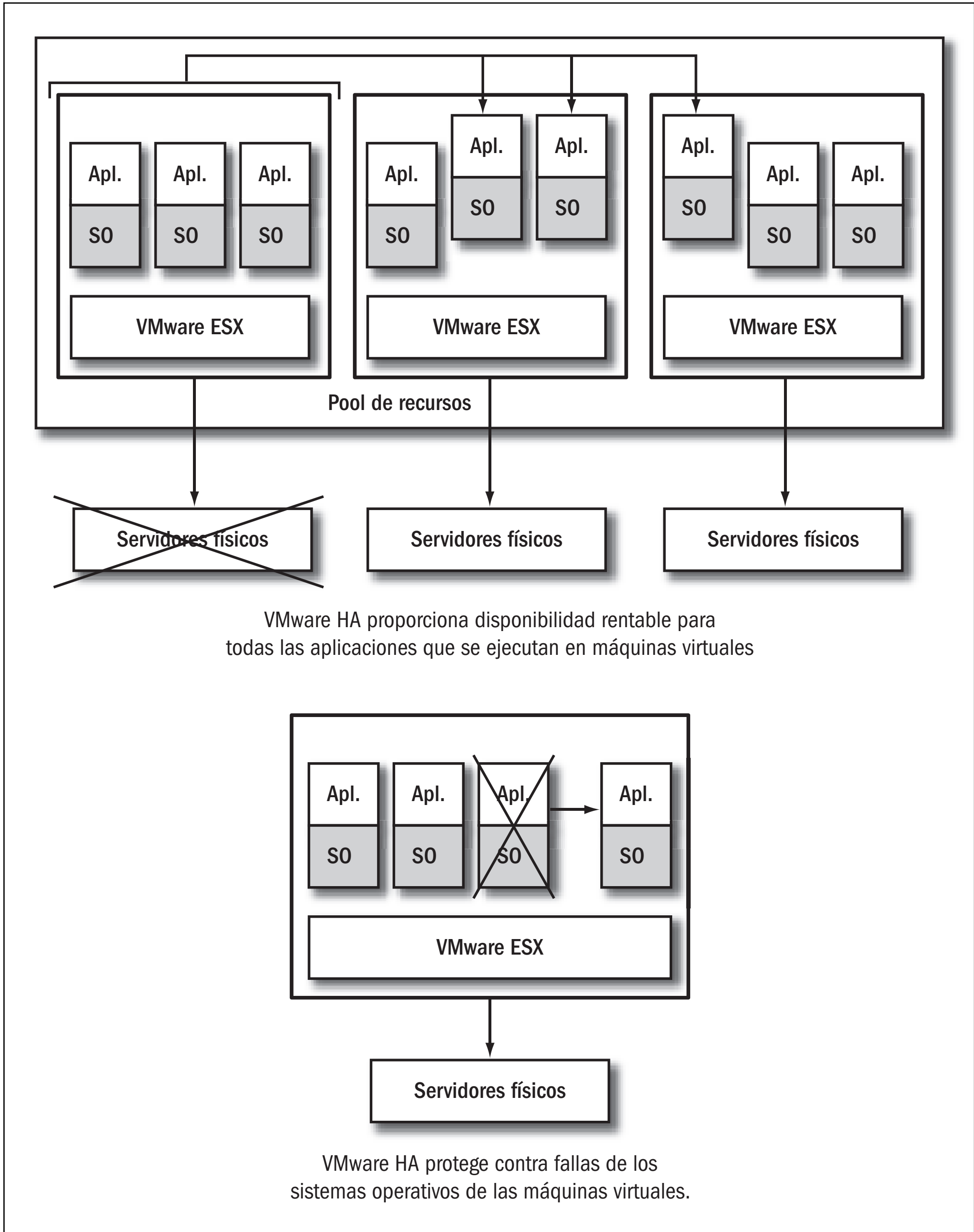


***Figura 5.** Si falla tanto un nodo ESX/ESXi como alguna máquina virtual, HA se ocupa de reiniciarlas para mantener al mínimo posible la pérdida de servicio.*

Ésta es una solución realmente económica, comparándola con las soluciones para sistemas operativos específicos, donde las licencias son pagadas por cada sistema. Esta solución puede configurarse para todos los servidores virtuales utilizando la misma licencia de uso y sin hardware adicional. También genera un

gran ahorro en lo que se refiere a la administración de un sistema de **failover**, debido a los conocimientos que esto requiere y a la complejidad que representa comparado con los sistemas tradicionales.
Podríamos dar esta ventaja de disponibilidad a servidores que no teníamos pensados como críticos, con esta acción tendríamos la posibilidad de entregarle robustez a toda la infraestructura y no sólo a los sistemas críticos. Debemos tener en cuenta que el servicio de HA de vSphere emplea un agente para monitorear los nodos ESX/ESXi y los servidores virtuales. Éste se instala en los nodos cuando habilitamos HA en el cluster, en tanto que en los servidores virtuales lo hace cuando instalamos las vmtools (VMware Tools). Este agente mantiene un **heartbeat** con los servidores pertenecientes a un pool de recursos.
HA es un sistema inteligente que monitorea a cada segundo el uso de capacidad, y siempre reserva espacio adicional para reiniciar las máquinas virtuales en otros nodos. Si esta capacidad no se contempla o se degrada, no se podrá seguir agregando equipos al entorno virtual de ese pool de recursos, y VMware no permitirá encender más servidores. También podemos configurar una prioridad de reinicio por cada servidor virtual. Algunos servidores son más críticos que otros y deben ser reiniciados en primer orden, y no tiene sentido reiniciar un servidor que no es crítico antes que uno crítico. Como vimos, debemos tener una tarjeta de red especial para utilizar vMotion. Veremos una opción específica que podemos habilitar para tener redundancia para los heartbeats y, también, redundancia en la administración de la consola de vSphere. El servicio de HA manda los heartbeats a través de la placa de red que se utiliza para administrar la consola, la cual tiene un switch virtual llamado Service Console. Es la primera placa de red que se configura al instalar ESX/ESXi; sin ella no podríamos administrar nada. Si esta placa de red se rompe por algún motivo, HA deja de enviar los heartbeats y manda a reiniciar las máquinas en otro nodo; también perdemos la administración del equipo, por lo que quedará inutilizable. Para que esto no suceda, ya que debemos configurar necesariamente la opción de vMotion, podemos utilizar esa placa de red con el objetivo de mandar los heartbeats hasta que arreglemos la placa en cuestión, con el agregado de que no perderemos la administración ni el balanceo de cargas que supondría tener un servidor apagado.



FAILOVER

Significa conmutación por error. Se refiere al cambio, al reemplazo del sistema que está en funcionamiento por otro igual a causa de algún error o falla. Debemos saber que este cambio se da sin intervención humana, automáticamente, para ofrecer alta disponibilidad. Utiliza un pulso de corazón que se manda por una conexión de red entre los equipos.

Detalles del sistema DRS

HA se complementa extraordinariamente con esta opción de DRS (*Distributed Resource Scheduler*). DRS balancea nuestra granja (cluster) de servidores entre los nodos para optimizar los recursos disponibles y no sobrecargar el hardware; asigna recursos según la demanda de los servidores virtuales y la saturación de los servidores físicos. Los recursos se agrupan en un pool, y puede haber uno o varios. Es posible priorizar también en el sistema de DRS las aplicaciones críticas ante las no críticas, siguiendo las necesidades del negocio de la empresa.

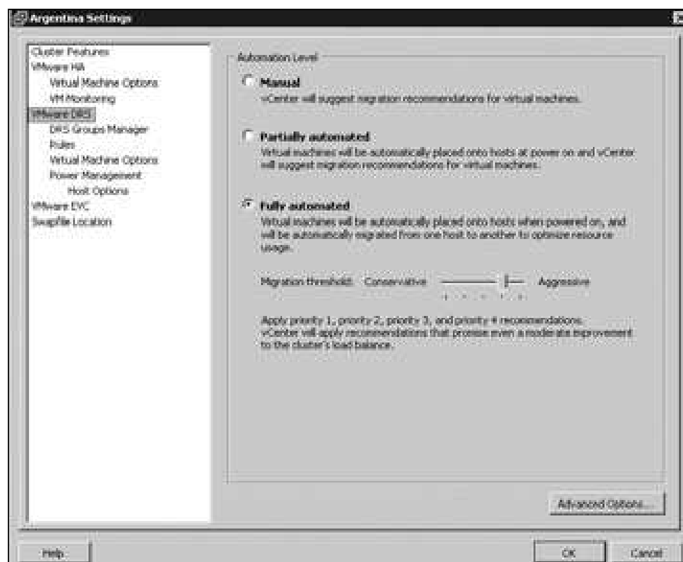


***Figura 6.** Vemos aquí las posibilidades que nos da DRS para funcionar. Cada una de estas opciones nos permitirá definir la forma en que vSphere nos entrega sugerencias sobre la migración.*

El servicio de DRS puede configurarse para que funcione de manera manual o automática. El modo manual sólo informará qué servidor recomienda mover y a qué nodo. Tiene varios niveles de recomendaciones y, según ellas, la forma automática puede ser más o menos agresiva. Al ser más agresiva, mueve más servidores y hace



DPM (DISTRIBUTED POWER MANAGEMENT)

Permite tener un gran ahorro de energía, que supera el 20% del consumo. Ésta es una función innovadora, que monitorea el uso de los servidores virtuales y el consumo de los recursos físicos. Cuando ve que la carga disminuye, reagrupa todos los servidores virtuales para apagar nodos ESX/ESXi innecesarios. Cuando la carga sube, los enciende automáticamente.

caso a más recomendaciones que si no fuese agresiva. Esto puede generar un gran desgaste para nuestro hardware si se está continuamente moviendo equipos virtuales; por eso se recomienda un nivel medio de agresividad para esta herramienta. El DRS funciona según reglas predefinidas en su configuración. A la vez, permite que un solo administrador maneje un gran pool de recursos y automatiza el mantenimiento de hardware. La capacidad de agregar nuevo hardware a la granja es muy simple: debemos configurarlo como los otros nodos y tan sólo agregarlo. Luego, el DRS se encargará de balancear las cargas entre todos los ESXs. Otra opción de DRS muy interesante es que podemos configurar la afinidad de los servidores virtuales, diciendo que uno pueda moverse en ciertos nodos o moverse en todos. DRS también trae una opción de **DPM** que aporta gran ahorro a la compañía.

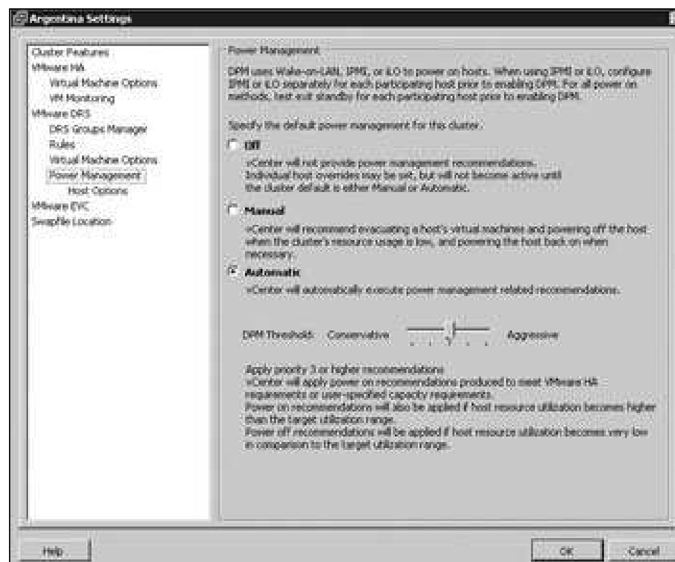


Figura 7. *El DPM puede estar apagado; podemos obtener recomendaciones; o, en modo automático, apaga y enciende los hosts según la demanda de recursos.*

Con la opción de DPM, VMware ofrece compatibilidad con las necesidades de la *Green Technology Wave*, u onda verde, movimiento que busca minimizar los consumos de energía para tener un planeta más limpio y conservar los recursos.

Conceptos de Fault Tolerance

Fault Tolerance es el arma letal de VMware ante todos los otros competidores. Es lo que resalta a vSphere en el mercado de las soluciones virtuales. Fault Tolerance debe configurarse de forma especial, al igual que Vmotion; es el mismo tipo de switch virtual (VMkernel), y también hay que tener una VLAN aparte, con una IP fija sobre ella. Cuando creamos el switch virtual, en vez de elegir el

casillero de Vmotion al colocar la dirección IP, elegimos el de Fault Tolerance. Debemos saber que cada uno de los nodo ESX debe tener una placa de red dedicada para este servicio conectada a Gbit. Al habilitarlo para un servidor, se creará una copia exacta del servidor objetivo, dejándola en modo pasivo. Así, tendremos dos copias iguales de un mismo servidor en distintos nodos ESX/ESXi. Ante cualquier interrupción que se produzca en el servidor objetivo, el pasivo tomará el control, al igual que sucede en un cluster físico. Esto nos brinda cero tiempo de bajada para cualquier servidor.

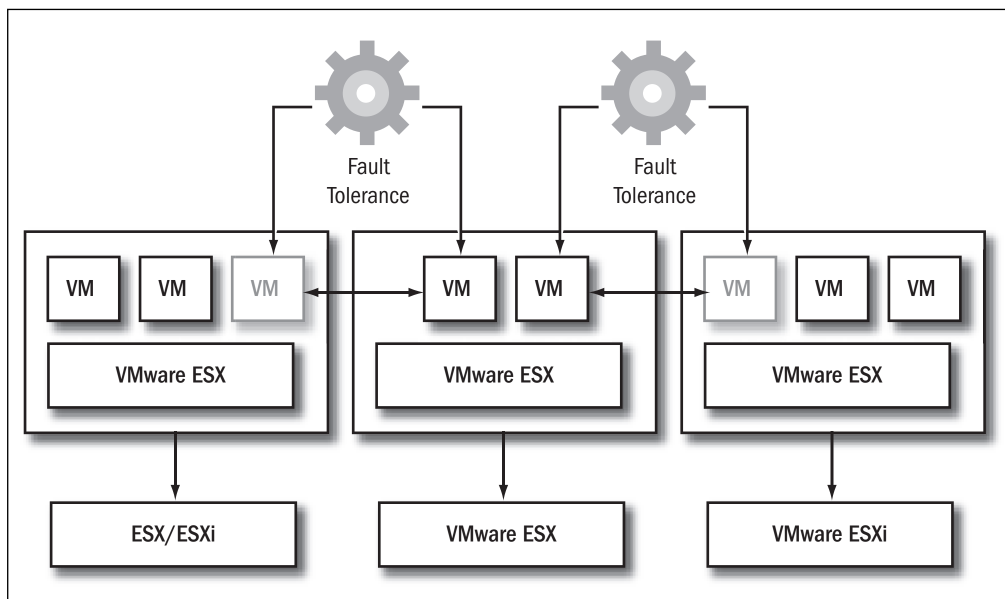


Figura 8. *Nuestra infraestructura virtual queda intacta ante un error de la infraestructura física. El sistema de Fault Tolerance no tiene comparación.*

Sin dudas, ésta es la mejor solución para nuestros sistemas, ya que elimina el tiempo de parada de los servidores. Esto significa alta disponibilidad real, 100% asegurada. Existen algunos prerrequisitos para implementar Fault Tolerance, y debemos tenerlos en cuenta antes de habilitar un servidor virtual con esta característica:

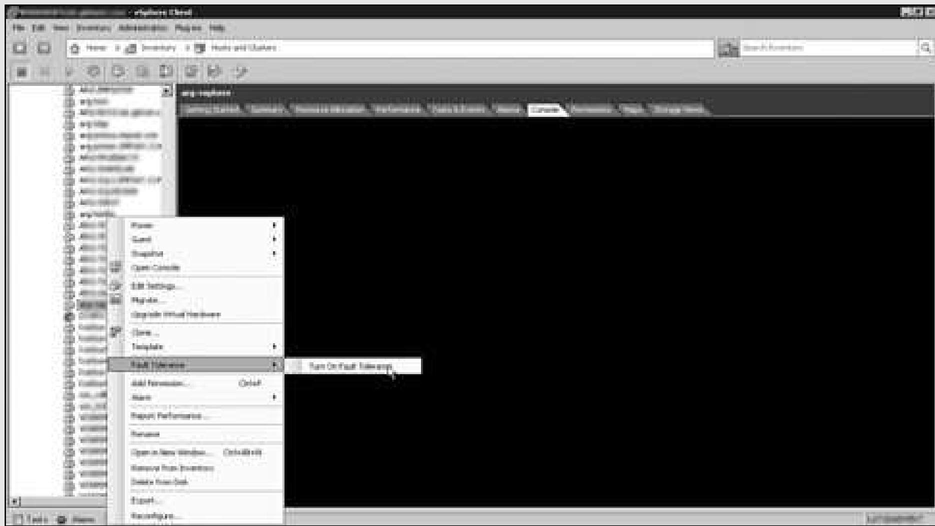
- Los nodos deben tener una instalación ESX versión 4.0 o superior.
- Es necesaria la existencia de un cluster HA.
- El servidor virtual no puede tener ningún CD, imagen o disco conectado.
- Debe estar en un almacenamiento compartido entre los nodos.
- El servidor virtual debe tener una configuración de discos thick. Un servidor con discos thin no podrá colocarse en Fault Tolerance.
- Debe tener una sola virtual CPU.
- El consumo de recursos aumentará un poco más.

- La opción de DRS se deshabilitará para el servidor virtual que obtenga la opción de Fault Tolerance, ya que lo torna innecesario.
- Es importante saber que no se pueden realizar snapshots o capturas; por lo tanto, no se podrán hacer backups del servidor correspondiente.
- No se podrá mover el servidor de LUN utilizando Storage Vmotion.

Luego de configurar la placa, si vamos a la solapa de **Summary** y nos ubicamos sobre un nodo ESX, aparecerá en la parte de las características generales un campo llamado **Host Configured for FT: Yes**. Esto nos mostrará que Fault Tolerance está configurado correctamente en el nodo. Luego faltará indicarle a algún servidor virtual que se coloque en Fault Tolerance.

Habilitar Fault Tolerance para un servidor virtual — PASO A PASO

1 Vaya a la consola de vSphere y, en el servidor que quiera proteger, haga clic derecho y elija **Fault Tolerance/Turn on Fault Tolerance**.

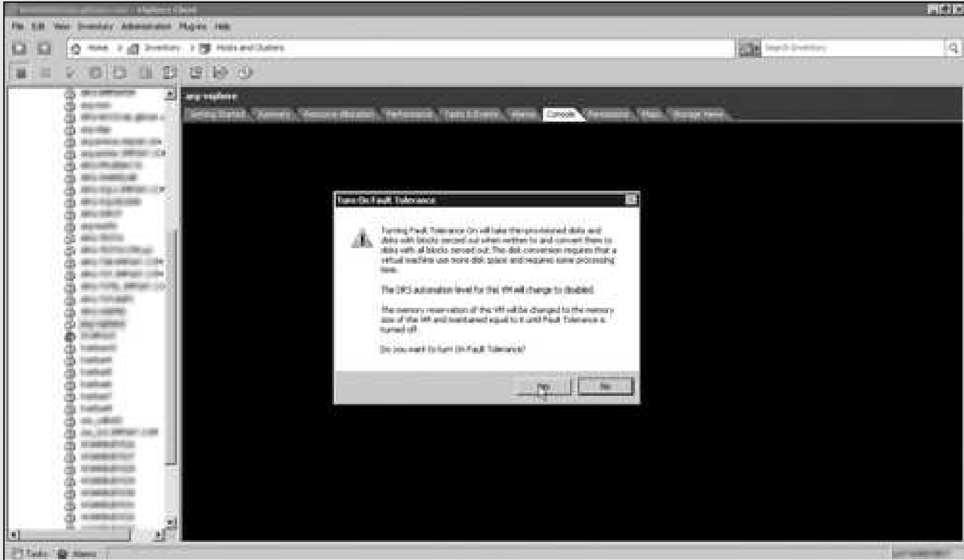


▶

MARC BENIOFF

Es actualmente el CEO de SalesForce y se recibió de Bachiller en Administración de Negocios en una universidad de California. Su libro favorito es de Tzu, llamado *The Art of the War*, muy recomendado en negocios y utilizado por varios CEOs. Está basado en la guerra de Vietnam y sus estrategias aplicadas a los negocios.

2 Para continuar este proceso deberá presionar en el botón denominado **Yes**, en el cuadro de diálogo donde se advierte que no tiene sentido tener el DRS activado para este servidor, por lo que se desactivará.



3 En este paso deberá tener paciencia ya que la tarea solicitada comenzará a desarrollarse. Siga su secuencia en el apartado denominado **Tasks** y, luego, verifique que, en la solapa **Summary** del servidor protegido, dentro del recuadro **Fault Tolerance**, diga **Protected**.



Las actividades se replican y coordinan entre el servidor objetivo y el pasivo gracias a una tecnología llamada **VMware vLockstep**. Ésta toma los servidores primario y secundario, y los hace ejecutar idénticas secuencias de instrucciones de sus plataformas. Captura todos los cambios a nivel procesador y a nivel de dispositivos de entrada y salida, y los replica. Estas réplicas de eventos no determinísticos se hacen a grandes velocidades, al estar conectados en una red de Gigabit. Al corromperse el servidor primario, el nodo ESX/ESXi mantiene las instrucciones que no se pudieron llevar a cabo en el servidor y habilita el secundario como primario para que continúe la operación. En ningún momento hay pérdida de datos o modificaciones. Luego, por HA, el primario que había fallado vuelve a reincorporarse a la granja, ahora sí, en el papel de secundario. Todo el proceso es transparente para los usuarios finales y totalmente automático, sin intervención de ningún administrador. Para que funcione vLockstep, es necesario que la CPU física de cada nodo tenga esa capacidad. VMware ha trabajado con empresas como Intel y AMD para que existan instrucciones especiales tendientes a usar esta tecnología. Es una extensión de instrucciones y las CPU de nuestros nodos deben ser compatibles para habilitar Fault Tolerance. Fault Tolerance puede fallar si queremos habilitarla en equipos virtuales con grandes discos o si el almacenamiento de los nodos es muy lento. Para habilitarla en estos casos necesitamos apagar el equipo, habilitarlo y, luego, volver a encenderlo; sin realizar estas tareas, será imposible habilitarlo.

Herramientas de actualización

Necesitamos actualizar los nodos ESX/ESXi, vSphere, el hardware virtual y, también, las VMware Tools instaladas en cada servidor virtual. Para hacerlo, contamos con una herramienta llamada **VMware Update Manager**. La secuencia de actualización correcta es actualizar vSphere, actualizar cada nodo, luego hacerlo con el hardware y, por último, con las herramientas para cada servidor. Esta herramienta también nos permite administrar las actualizaciones de los sistemas operativos virtuales, centralizando la instalación de parches. Éstos se bajan a vSphere y después se distribuyen para todos los servidores virtuales. También podremos actualizar Virtual Appliances y software de terceros. Al momento de actualizar vSphere, se modifican las bases de datos, la estructura y los datos que contenga. Podemos optar



ACTUALIZACIÓN DE ESX 3.5 A 4.1

Las versiones 3.5 no pueden administrarse con vSphere 4.1. Para hacerlo, tenemos que instalar desde cero los nodos ESX con la nueva versión de ESX/ESXi 4.1. Es por eso que VMware ofrece una herramienta llamada **vSphere Host Update Utility**, porque no se pueden actualizar con Update Manager al no poder conectarlos contra la consola.

por actualizar nuestro servidor ya instalado o instalar todo desde cero. Esta última opción es la más limpia y la más adecuada. En la actualización de sistemas que llevan una base de datos y un cambio en su estructura, generalmente queda basura dando vueltas en las tablas, registros que no están completos por no tener todos los campos de las nuevas modificaciones porque al crearse no existían. Entonces, lo mejor es hacer borrón y cuenta nueva. Esto es un poco más arriesgado si tenemos muchas configuraciones particulares que serán borradas, pero nos ahorraremos muchos dolores de cabeza. Entonces, podemos utilizar vSphere Update Manager o quemar la imagen ISO de la nueva versión y efectuar una nueva instalación.

Si actualizamos los nodos con vSphere Host Update Manager, la herramienta instalará todo desde cero. Su uso es rápido y sencillo. Se muestran los nodos con sus versiones, y con una imagen podemos actualizar todos desde el servidor vSphere. Al abrir la aplicación, aparece un mensaje para ver si queremos buscar actualizaciones desde el repositorio; luego debemos elegir si queremos hacer un escaneo de posibles actualizaciones para el equipo. Entonces, además de actualizar la versión de ESX/ESXi, se actualizarán todos los parches hasta la fecha, de modo que no tengamos que hacerlo luego. Una vez que actualizamos los nodos, ya podemos conectarlos en la consola de vSphere. Para actualizar un nodo ESX/ESXi, si es versión 4.0, por ejemplo, podemos realizarlo con Update Manager. Debemos apagar las máquinas virtuales o pasarlas a otro nodo. Después de actualizar los nodos, pasamos a la actualización de los servidores virtuales. Principalmente, tendremos que actualizar hardware virtual y Vmtools. El hardware virtual puede actualizarse con el equipo apagado. Hacemos clic derecho y elegimos **Upgrade Hardware**.

Otra posibilidad es realizar todas estas actualizaciones con VMware vSphere Update Manager. En este caso, se organiza el workflow (flujo de trabajo) de actualización y se va actualizando todo en forma programada. Es bastante complejo actualizar toda la infraestructura así, y es preferible hacerlo paso a paso. Entonces, usaremos este método sólo para instalar parches en los ESX/ESXi. Update Manager se instala como un plugin más de la consola vSphere. Una vez listo, aparecerá un icono en la home de vSphere llamado Update Manager. Desde allí, ingresamos a configurar todas las particularidades de la herramienta. Luego, en cada servidor virtual y cada nodo habrá una solapa de Update Manager para configurar opciones de esos equipos en particular.

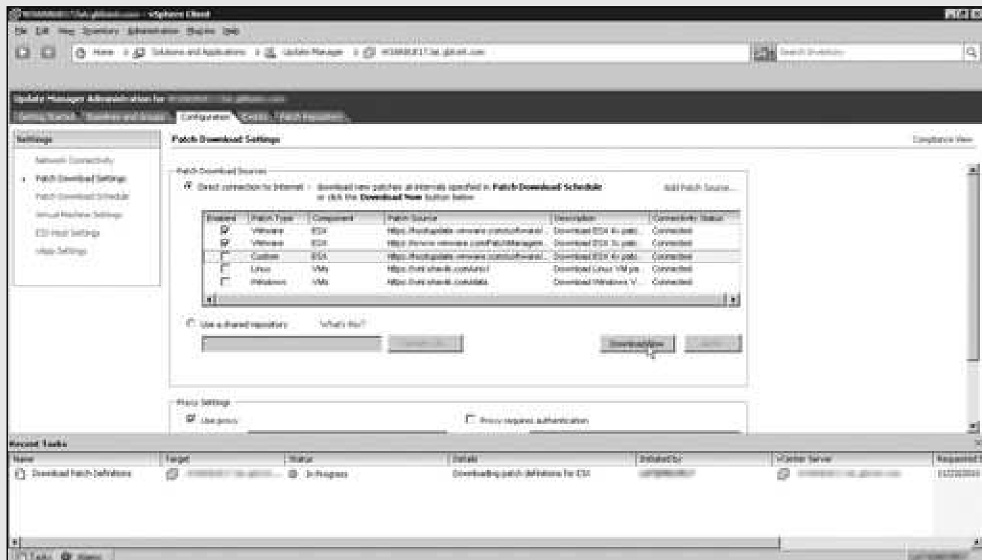


MAINTENANCE MODE

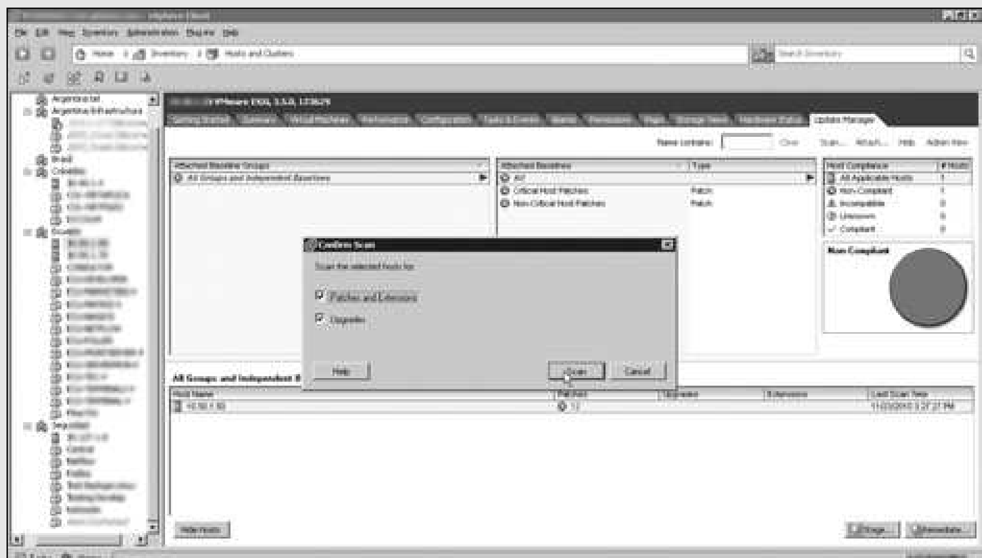
Esta opción se utiliza para realizar mantenimiento en servidores ESX/ESXi. Se puede colocar el estado del servidor con un clic derecho, pero se deben trasladar todas las máquinas virtuales. Si el storage es muy lento, no podrá hacerse automáticamente, sino que deberemos hacerlo de a uno y, luego, habilitar la opción para trabajar.

Realizar un update de un nodo ESX/ESXi — PASO A PASO

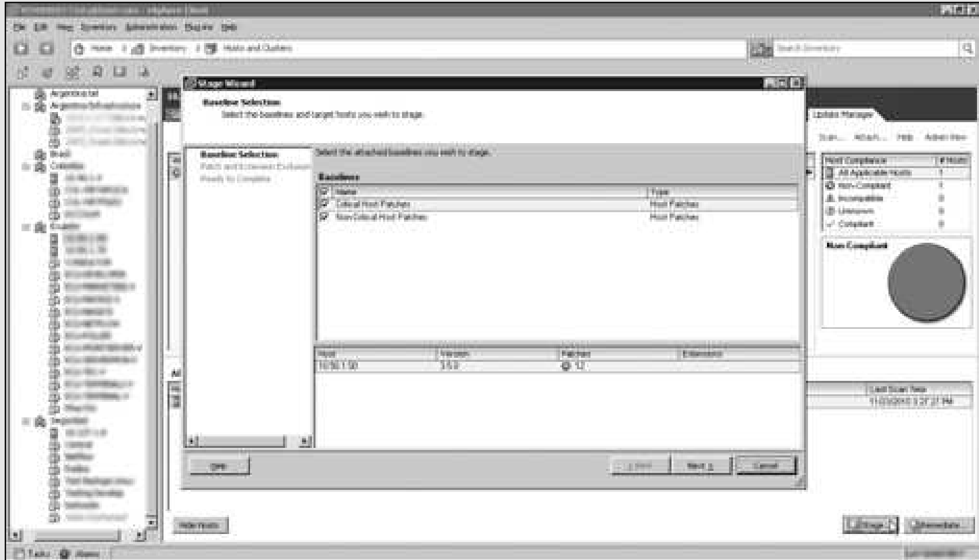
1 En la home de la consola de vSphere, oprima el botón de Update Manager para abrir la consola de Upgrade. Vaya a la solapa **Configuration**, verifique los parches que desea obtener y oprima el botón **Download now**.



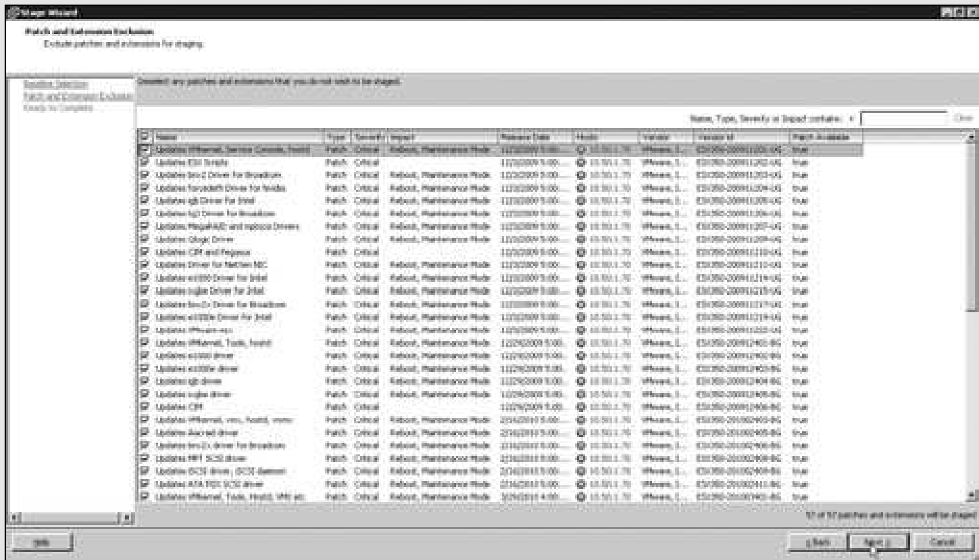
2 Diríjase al host que quiera actualizar, vaya hasta la solapa **Update Manager** y, luego, haga clic sobre el link **Scan...** Marque las dos opciones y oprima **Scan**.



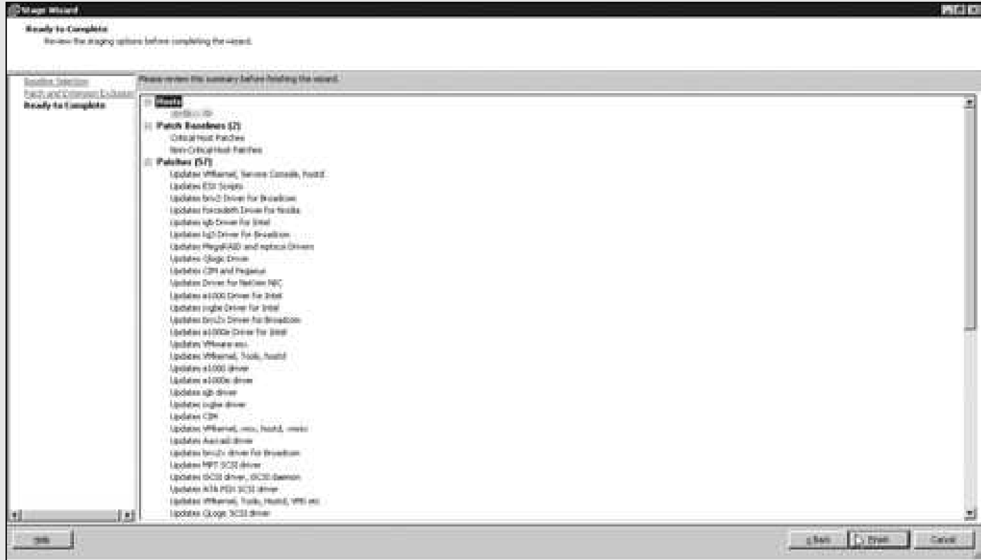
3 Verifique los detalles de los parches que necesita instalar en el host y oprima **Stage...** para comenzar a copiar los archivos. En la ventana elija los parches críticos y los no críticos, y pulse sobre la opción **Next**.



4 Para continuar, elija uno por uno los parches que desea instalar. Es importante que realice una revisión de las características correspondientes a cada uno de ellos. Luego deberá marcar los correctos y hacer clic sobre **Next**.



▶ 5 Vea el resumen y presione el botón **Finish**. Cuando pueda, mueva los equipos virtuales y posteriormente reinicie el host; más tarde diríjase a la misma solapa y pulse sobre la opción llamada **Remediate...**.



Esto es todo lo que debemos saber para administrar las actualizaciones para el sistema vSphere. Debemos tener en cuenta que las actualizaciones de software de terceros son particulares de cada fabricante.

Es importante saber que las actualizaciones correspondientes a los sistemas operativos no se eligen en el Paso a paso mostrado anteriormente porque, en general, las empresas cuentan con sistemas mucho más completos y particulares, que tienen un mejor funcionamiento y administración centralizada.

Podemos señalar que una de las herramientas relacionadas con la actualización es la denominada System Center Configuration Manager, la cual analizaremos con más detalle en el siguiente capítulo de este libro.



VLOCKSTEP

Este servicio creado por VMware mantiene sincronizadas las operaciones en un cluster protegido por Fault Tolerance. Permite la réplica de operaciones de entrada y salida a nivel instrucciones de BIOS, gracias a las extensiones de los microprocesadores AMD e Intel con sus tecnologías especiales para el uso de VMware.

BACKUPS DE AMBIENTES VMWARE

Ya conocimos todas las capacidades que nos dan los ambientes virtuales y sus grandes beneficios, pero ¿qué pasaría si por algún motivo un servidor virtual dejara de funcionar? Supongamos que uno falla: entonces, debemos tener alguna copia de resguardo para realizar una rápida recuperación. Existen algunos métodos de backup que veremos en esta sección, y también conoceremos qué son los snapshots (fotografía) de un servidor virtual y cómo administrarlos.

Qué es un snapshot

Es importante mencionar que hace sólo algunos años, con la existencia de los servidores físicos era impensable pensar en un snapshot. Lo más parecido que existía en ese momento era un equipo en spare, pero nada más que eso.

Para entender qué es un snapshot podemos decir que se trata de algo así como tomar una foto del servidor en un instante determinado. Así, se podría crear un equipo virtual para entrega de un servidor de testing, instalar el sistema operativo y tomar un snapshot (snap_testing). Luego, podría instalarse una base de datos, configurar la administración, tomar un snapshot y entregar el sistema a quien lo haya pedido (snap_DB). Después, se puede volver al primer snapshot tomado (snap_testing), donde sólo teníamos el sistema operativo instalado, y si nos piden un servidor de correo, podríamos instalar el servicio y así crear otra rama de snapshot (snap_correo); podemos ver que esta forma de trabajar nos proporciona un considerable ahorro de tiempo y recursos. Más tarde, supongamos que nos piden otra vez un servidor de base de datos (snap_DB). Podríamos volver al snapshot que teníamos de él y continuar desde allí, dejando sin efecto el de correo. Es importante no incurrir en el error de tener varios snapshots sin uso, ya que desaprovecharíamos el espacio en disco.

Los snapshots conservan varios estados de las máquinas virtuales; entre los datos que se guardan, tenemos el estado de la memoria, el estado de los discos, la configuración de la máquina virtual y los datos del BIOS. Los snapshots son muy importantes en la creación de backups, ya que las herramientas de respaldo los crean para tomar la copia y, así, separar la demanda de la red, del equipo productivo.



SNAPSHOT

Los snapshots son fotografías del estado de un equipo en un momento; algo parecido a un punto de restauración pero mucho más potente, ya que nos permite ir y venir en un árbol de descendencia. Podemos tener varios puntos en el tiempo y volver a ellos. Esto se asemeja a viajar en el tiempo de vida del servidor, con la posibilidad de tener varios finales.

Soluciones de backup

Este proceso implica realizar una copia de los archivos de los servidores virtuales a otro medio de almacenamiento, que puede ser cinta de backups, memoria flash o disco compacto. Por supuesto que existen herramientas creadas para este fin. Por lo general, el proceso abarca crear un snapshot del servidor virtual y trabajar el backup con ese snapshot mientras el servidor objetivo sigue su rumbo independientemente. El backup puede realizarse mediante scripts, soluciones de terceros o soluciones de la empresa VMware. Obviamente, los costos en cada caso serán distintos. VMware ofrece varias soluciones de backup, y una de ellas es **VMware Consolidated Backup**. Esta herramienta plantea un escenario en donde se instala un servidor de backup con la solución de resguardo de la empresa y otro que hace el papel de proxy de backups. Este servidor de backup proxy tiene un ESX. El proceso es el siguiente. Se crean snapshots desde el storage de la granja productiva hacia el storage del servidor proxy de backup. Los jobs (trabajos de backups) se generan en la consola de vSphere y son redireccionados al servidor de proxy de backup. Pueden ser full o incrementales, se pueden configurar muy fácilmente y hasta pueden programarse con una ventana de backup. El snapshot de un servidor virtual recién tomado se monta en el servidor ESX, y se toma el backup del equipo proxy con los agentes del fabricante que la empresa tenga en uso. Por último, se desconectan y se borran los snapshots tomados. Es una buena solución, pero requiere una licencia bastante cara y otro servidor físico.

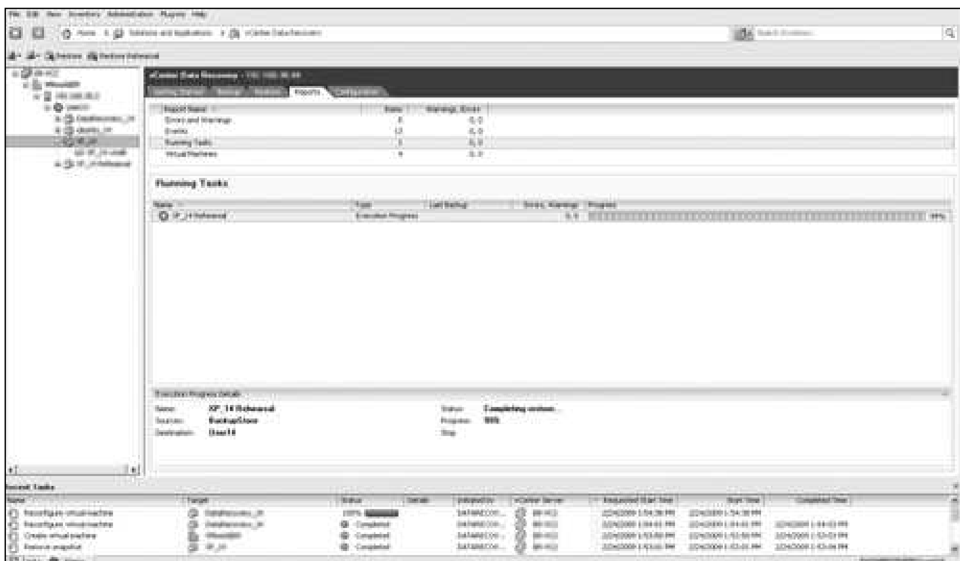


***Figura 9.** La consola de Data Recovery es muy parecida a la de vSphere. Se distribuye de forma similar, pero posee otras herramientas y distinta estructura.*

Una solución algo más reciente es **VMware Data Recovery**, que no sólo hace backups de los ESX y sus servidores virtuales, sino que también permite recuperar

archivos específicos dentro de los servidores virtuales, algo que en otras opciones no es posible. La solución se compone de un plugin que se instala en la consola de vSphere, un virtual appliance de VMware Data Recovery y un storage con capacidad de reduplicación. En sí es similar a la solución de backup explicada anteriormente, pero funciona con un appliance, con las ventajas que eso significa. Los snapshots pueden tomarse y moverse a la virtual appliance para no comprometer la placa de red del servidor virtual que se va a resguardar. Al recuperar un servidor virtual que falló, Data Recovery suplanta la máquina virtual por un punto de restauración del backup. Esto es muy eficiente, porque copia sólo el fragmento de bloques que han cambiado. Los backups y las restauraciones de archivos específicos son similares, pero deben administrarse desde la consola dentro del servidor virtual con un cliente que se instala. En tan sólo cuatro pasos, es posible administrar los backups y configurarlos de manera automática. Únicamente hay que seleccionar el servidor objetivo, elegir el storage destino y un calendario de backups, y seleccionar una política de retención.

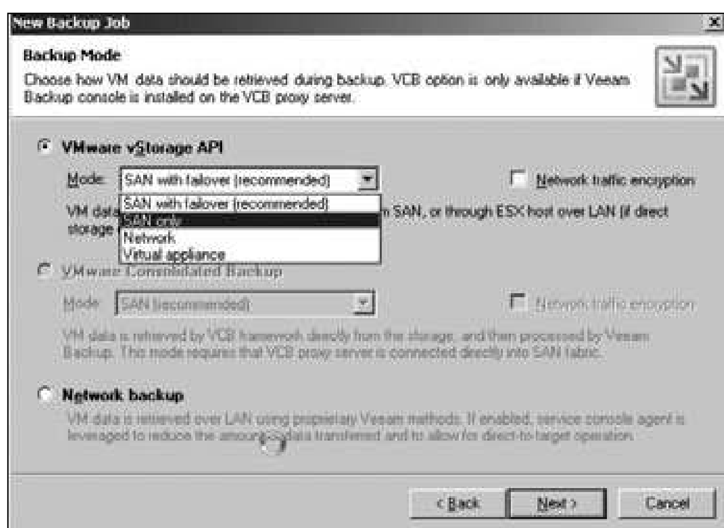


***Figura 10.** La consola también es muy similar a vSphere, pero se agrupa de manera muy distinta; se parece más a la consola de Veritas NetBackup.*



SLA (SERVICE LEVEL AGREEMENT)

Debemos saber que SLA es un contrato escrito de aseguramiento de nivel de servicio. Lo entrega el prestador del servicio a su cliente y debe cumplirse a rajatabla lo que dice allí. Se trata de una herramienta importante ya que permite determinar una calidad de servicio, tanto para el prestador como para el consumidor. Crea un consenso entre las partes.

Hay otras soluciones en el mercado, como la de la empresa **EMC** o la más conocida, **Veeam Backup**. Esta última es la más popular y la que más evoluciona día a día. En su última versión, permite recuperar el servidor virtual corriéndolo directamente desde sus archivos de backup. También permite hacer backups de archivos de cualquier aplicación virtualizada, e incluye una herramienta llamada **SureBackup**, que analiza si el backup realizado es recuperable o no. Cuántas veces nos habrá ocurrido que se nos rompe algún equipo, contamos con un backup hecho y confiamos en él, y cuando vamos a utilizarlo, éste no funciona. Esta herramienta evita esa situación tan desastrosa.

Backup con Symantec Veritas NetBackup

Hay empresas en las que la solución de Symantec es muy utilizada para realizar backups de equipos Windows y Linux. La extensión de la licencia para efectuar resguardos de equipos VMware es demasiado costosa, al igual que las licencias de VMware para sus soluciones. Entonces, como detallamos antes, el procedimiento consiste en utilizar scripts para realizar los snapshots, copiarlos a otra ubicación, configurar los backups con las ventanas adecuadas y, posteriormente, proceder a realizar la eliminación de los archivos que sean innecesarios.

Debemos tener en cuenta que esta solución es un tanto complicada para usuarios que no posean conocimientos avanzados, ya que requiere que se realice la intervención mediante línea de comandos. También necesita una coordinación de tiempos para el script programado que hace el snapshot, el job de backup para que copie los archivos y el script programado para que se encargue de eliminar los archivos de los snapshots no utilizados. Hay muchas formas de realizar el script que no veremos en este libro, ya que van más allá de su propósito.

Entonces, debemos saber que es necesario realizar la programación de los scripts en cada nodo para hacer los resguardos de todos los equipos y de esta forma desarrollar una política de backups para cada nodo en la consola de Veritas correspondiente. Para hacer la restauración de alguna máquina que haya fallado, debemos saber en qué equipo estaba corriendo a la hora de hacer el backup, porque puede ser que figure en otro nodo si se aplicó DRS por alguna razón.

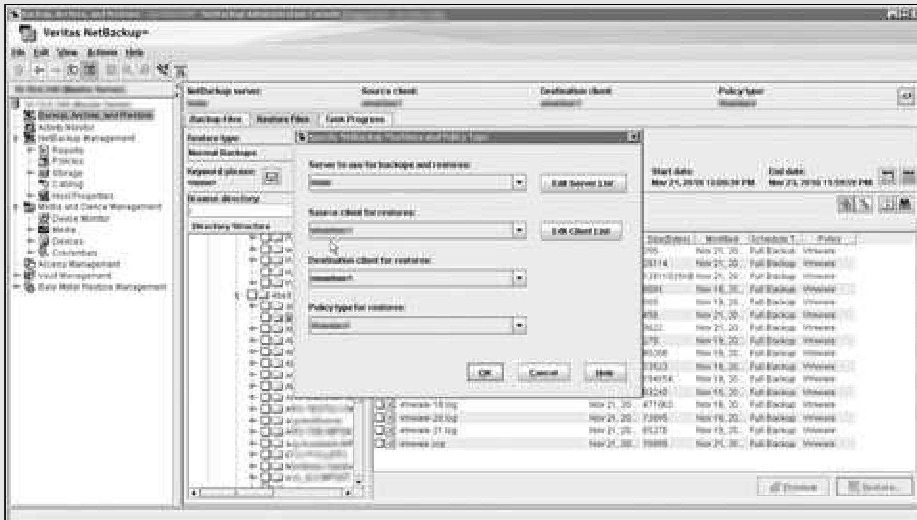


LICENCIAS DE ESX/ESXI

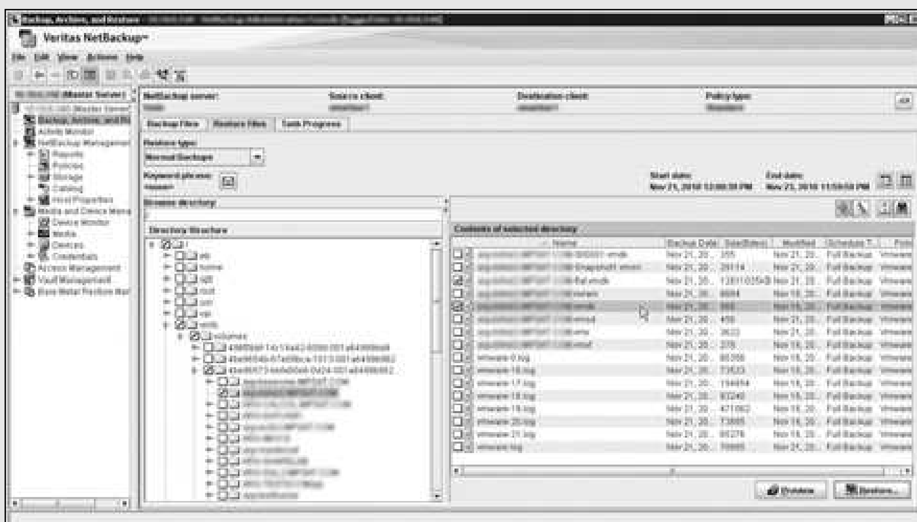
Estas licencias de ESX se dan por microprocesador y por core, es un mix. Si nuestro servidor físico tuviese dos microprocesadores quad core, necesitaríamos dos licencias de 4 core para poder instalar un ESX. Por el contrario, las licencias de los ESXi son gratuitas y son el futuro del sistema de vSphere por ser un código cerrado, donde no pueden intervenir terceras partes.

■ Restaurar el backup del servidor virtual PASO A PASO

1 Conéctese al servidor de backup y vaya hasta la opción **Backup, Archive and Restore** del menú izquierdo. Luego, en la solapa **Restore** elija los servidores y una política. Oprima sobre la opción denominada **Ok**.

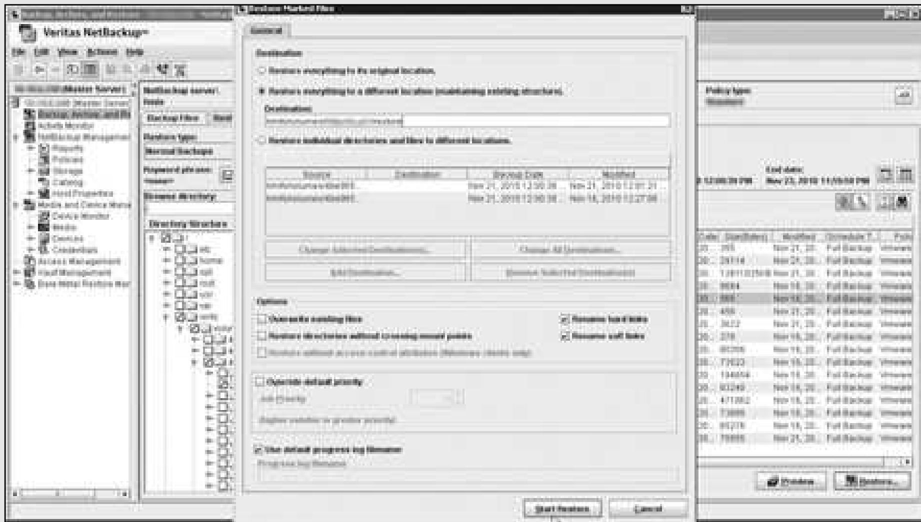


2 Elija la fecha del backup y, al abrirlo, recorra el árbol y vaya hasta la carpeta **/vmfs/volumes/key_del_volumen/nombre_servidor_virtual**. La key será la que creó el sistema. Seleccione el archivo **vmdk** más pesado y el otro archivo **vmdk** del mismo nombre, pero sin la extensión **–flat**.

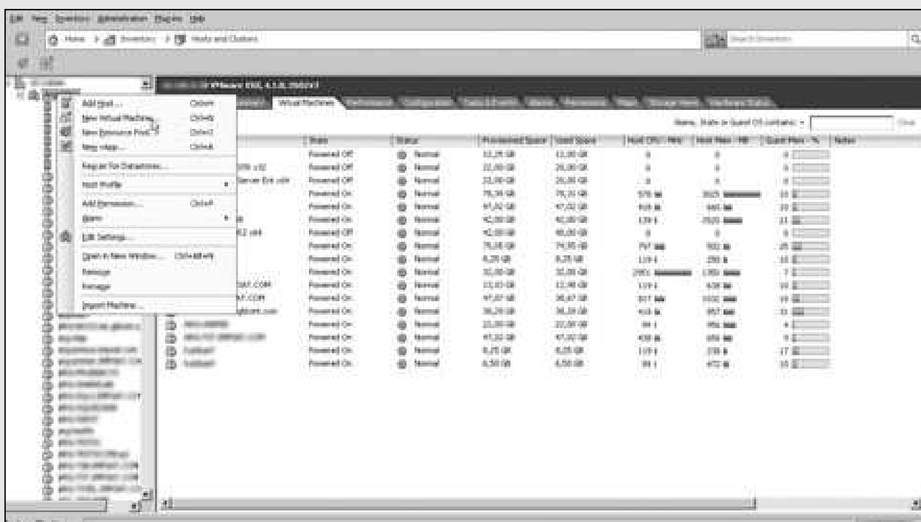


▶

3 En este paso deberá elegir la opción denominada **Restore everything to a different location**. Luego de hacerlo ingrese otra ubicación para los archivos de restore; por ejemplo, puede usar la siguiente: **/vmfs/volumes/key_del_volumen/restore**. Haga clic en **Start Restore**.



4 Espere mientras la operación se lleva a cabo. Cuando el proceso de restore haya terminado, vaya hasta la consola del sistema vSphere y ejecute las acciones necesarias para crear una máquina virtual nueva en modo **Custom**. Siga cada una de las indicaciones entregadas por el asistente.



▶

▶

5 Al elegir el disco, seleccione la opción de **Use an existing virtual disk** para elegir el disco restaurado.



6 Elija el datastore donde se encuentra la carpeta de restore y, luego, siga los pasos para terminar de crear la máquina virtual.



La creación de esta máquina virtual genera una carpeta de archivos nueva con el nombre del servidor nuevo; si suponemos que se llama **Servidor_custom**, la carpeta se ubicaría en **/vmfs/volumes/key_del_volumen/servidor_custom**. Debemos mover

los archivos de la carpeta restore hacia esta carpeta y renombrarlos para que queden bien. Podemos utilizar el browse datastore o, desde la línea de comandos, utilizar el siguiente comando ubicados en **/vmfs/volumes/key_del_volumen**:

mv restore/nombre_servidor_virtual servidor_custom/

Por último, modificamos el archivo VMX de la máquina virtual. Modificamos la línea **scsi0:0fileName** y colocamos la ubicación nueva de los archivos. Ahora sí, podemos encender el servidor virtual restaurado.



***Figura 11.** En el sitio web **www.symantec.com/es/mx/business/netbackup** encontraremos más información acerca del funcionamiento de Symantec NetBackup.*

... RESUMEN

Cerramos la implementación de VMware vSphere, la herramienta líder en el mercado de virtualización. Vimos cómo instalar un servidor vSphere, la manera de anexarle nodos ESX/ESXi, la implementación de varias características que ofrece y Fault Tolerance. También vimos cómo crear snapshots y las particularidades de los sistemas de backup. vSphere es una herramienta muy poderosa, que cambió la forma de los datacenter, redujo equipos y nos hizo considerar los servidores como objetos muy maleables.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 Enumere las características especiales de vSphere.

2 Describa en detalle cómo se crea un cluster en vSphere.

3 ¿De qué forma se conectan los nodos ESX con vSphere?

4 ¿Qué es Vmotion y para qué sirve?

5 ¿Qué es Storage Vmotion? ¿Cuál es la diferencia con Vmotion?

6 Describa las características del sistema de HA y DRS.

7 ¿Qué es Fault Tolerance y por qué es tan importante?

8 Describa qué es un snapshot y la manera de obtenerlo.

9 ¿Qué es VMFS y qué diferencia hay con los sistemas de archivos tradicionales?

10 Enumere y describa las distintas formas de backup que se mencionan en este capítulo.

EJERCICIOS PRÁCTICOS

1 Instale un servidor vSphere y conecte dos o tres nodos ESX/ESXi con un almacenamiento en común.

2 Configure las características de HA y DRS, y compruebe su funcionamiento desconectando la fuente de energía de un servidor ESX.

3 Cree algunos servidores virtuales con distintos sistemas operativos, e implemente las operaciones de Vmotion y Storage Vmotion. El Storage Vmotion puede realizarse entre el almacenamiento compartido y el local a cada servidor.

4 Implemente Fault Tolerance para algún servidor virtual.

5 Configure alguna solución de backup y pruebe a hacer un recupero de un equipo virtual.

System Center Configuration Manager

Los virus son una amenaza por más que ya hayamos destruido la preocupación debido al hardware. Los equipos se conectan a Internet y a la intranet, y siguen estando expuestosa infectarse en cualquier momento. La instalación de parches de software es el principal muro contra estas amenazas. SCCM nos da una mano frente a este problema.

MICROSOFT SYSTEM CENTER

Para administrar nuestra infraestructura al máximo, necesitamos obtener reportes de todo tipo, y automatizar configuraciones e instalaciones. Hay situaciones que se repiten a cada momento; instalaciones de software, modificaciones de sistemas y procesos de negocios que cambian prioridades, etc. System Center pone a nuestra disposición varias herramientas para crear infraestructuras dinámicas y autogestionadas, con el considerable ahorro de dinero y tiempo de administración que eso significa. Permite a los sectores de IT adaptarse rápidamente a las demandas del negocio según sus requerimientos.

Qué es Microsoft System Center y sus soluciones

System Center de Microsoft es un grupo de aplicaciones que permite crear infraestructuras dinámicas y autoadapatables. Con él obtendremos conocimientos de nuestra empresa que serían imposibles de lograr de otra manera, como información sobre infraestructura, políticas, procesos y buenas prácticas. Tendremos el control del parque de máquinas de escritorio, de servidores y otros dispositivos, todo en una sola aplicación. Los dispositivos pueden ser físicos o virtuales, y tener distintos sistemas operativos, no necesariamente Windows, sino también soluciones para sistemas UNIX y Linux, por ejemplo.

La visión de Microsoft de la IT dinámica se centra en dos campos esenciales: el **datacenter dinámico** y los **escritorios dinámicos**. Las soluciones de datacenter pueden ayudar a reducir los gastos de integración entre el negocio y los servicios del datacenter, para que pueda cumplir con sus contratos de **SLA** (*Service Level Agreement*) o **acuerdo a nivel servicio**, sin pérdida de capital. Las soluciones de escritorios dinámicos permiten ofrecer el acceso a los servicios IT, aplicaciones y recursos corporativos de una manera más ágil. Estas últimas ofrecen aplicaciones virtualizadas y en streaming con la consistencia y el rendimiento requeridos por los usuarios. Podremos administrar las máquinas de escritorio en forma remota y hasta distribuir un sistema operativo de acuerdo con las políticas de la empresa de manera estándar. Los productos de System Center son varios, cada uno especializado en cierto campo de IT. Ellos son:



IT DYNAMIC

Es una visión de Microsoft desde el año 2007 para proporcionar tecnologías críticas que permitan a empresas de IT y de desarrollo concentrarse más en sus estrategias y negocios. Pretende implantar una infraestructura dinámica para brindar agilidad al responder rápidamente a las demandas del negocio y mejorar así nuestros servicios.

PRODUCTO	DESCRIPCIÓN
System Center Configuration Manager	Permite tener un departamento IT más efectivo, escalable y seguro en entornos virtuales y físicos. Ofrece administración total de servidores, máquinas de escritorio y dispositivos móviles.
System Center Operations Manager	Es la herramienta principal para administración y monitorización de servicios en la empresa, principalmente, en ambientes Windows, porque funciona de forma trasparente con las aplicaciones.
System Center Data Protection Manager	Da protección y escalabilidad a nivel corporativo. Protege de forma unificada a servidores Windows, como SQL Server, Exchange, Share Point y otros.
System Center Virtual Machine Manager	Permite gestionar el ambiente virtualizado unificando las herramientas de Microsoft y de otros competidores, como VMware.
System Center Essentials	Brinda soluciones a organizaciones de tamaño medio, y permite realizar tareas de administración complejas en servidores físicos y virtuales, eficientemente.
System Center Service Manager	Permite administrar las necesidades del soporte técnico. Prevé nuevos incidentes, problemas, control de activos y administración de cambios.
Opalis	Proporciona procesos de automatización de respuesta a incidentes, aprovisionamiento, administración del ciclo de vida virtual y de cambios de procesos de IT, permitiendo cumplir con normas ITIL en la empresa. Se integran herramientas de System Center con las de otros fabricantes.
SoftGrid Application Virtualization	Permite administrar aplicaciones virtuales y convertir otras físicas en virtuales, para optimizar el uso de los recursos y compartir el cómputo de los servidores.

Tabla 1. *Subproductos de Microsoft System Center.*

Estas herramientas tienen una curva de aprendizaje muy rápida y permiten obtener notables resultados en poco tiempo. Proporcionan un bajo costo total de la propiedad (**TCO**) y un alto retorno de la inversión (**ROI**). Muchas de las soluciones de Microsoft están optimizadas para integrarse con System Center, los nuevos sistemas operativos Windows Server 2008 y Windows 7, a los cuales se da mayor control de políticas, normas y configuración. Una de las aplicaciones más importantes es Microsoft System Center Configuration Manager, en la que se centra este capítulo.

System Center Configuration Manager 2007 R2 (SCCM)

SCCM nos ayudará a optimizar nuestra infraestructura y volverla ágil, al automatizar varios aspectos nunca antes pensados. Se encarga de agrupar varias herramientas anteriores de Microsoft, como Microsoft Deployment Toolkit (MDT), Windows Server Update Services (WSUS), y otras.

Permite tener el control de la configuración de los activos de la empresa, y manejar todos los servidores, máquinas de escritorio y dispositivos móviles. Entre las funciones más importantes podemos mencionar:

- Buscar, administrar y desplegar parches de software a toda nuestra empresa, a nivel corporativo. Podremos llevar un control de instalación y reparación de errores si es que se presentan.
- Distribuir software de todo tipo. Podremos autoinstalar este software de forma urgente o programada, así como también mediante scripts, o sólo publicarlos para que los usuarios los instalen desde una lista.
- Desplegar sistemas operativos estandarizándolos en toda la empresa con las normas de seguridad correspondientes y los programas permitidos, con lo cual obtendremos un mayor control de los activos y las licencias.
- Obtener informes de todo tipo, detalles de las máquinas y de usuarios en línea. Los detalles son informados mediante una serie de acciones muy coordinadas que alimentan una base de datos de conocimiento empresarial, con la cual se los crea.

Debemos tener en cuenta que SCCM se basa en una infraestructura entre varios servidores y clientes instalados en los distintos dispositivos: servidores, equipos portátiles y de escritorio. Hay grandes cantidades de datos en nuestra empresa, y sólo SCCM puede convertirlos en muy buena información.

CÓMO INSTALAR SCCM

A continuación, aprenderemos a instalar SCCM en nuestra empresa para así adquirir el control de los sistemas y generar la información tan buscada por los gerentes, administrar, distribuir e instalar software y parches de una manera sencilla y centralizada. La instalación es muy simple, pero requiere manejar varios conceptos que iremos desarrollando a través de las secciones siguientes. Comenzaremos por ver los prerrequisitos, y continuaremos con la infraestructura, los roles de los servidores y la instalación propiamente dicha.

Prerrequisitos de SCCM

Hay varias herramientas que debemos instalar antes que SCCM. Necesitamos tener una base de datos y un sitio web. Los programas que precisamos instalar son:

- .NET Framework
- MSXML
- WSUS
- SQL Server 2005
- ISS, donde habilitaremos Bits, Asp y WebDav
- Publicar el nombre de nuestro SCCM

Debemos saber que .NET es necesario al igual que cualquier aplicación de Microsoft. Es esencial para poner a funcionar SCCM. MSXML es la versión XML de Microsoft, también primordial como .NET. WSUS es la herramienta administradora de parches de seguridad. Debemos tener en cuenta que SQL Server es necesario para realizar la instalación de la base de datos, que puede estar en el mismo servidor o en otro, dependiendo de nuestras expectativas de crecimiento. También debemos saber que el último prerrequisito es para asegurarnos de que todos los dispositivos conozcan el nombre del SCCM. Es posible lograr esta tarea de dos formas: la más recomendada es ampliar el schema del dominio con el cual se crea un registro DNS, pero también podremos publicarlo por WINS.

El CD de instalación trae una aplicación que simplificará el análisis de los cumplimientos de estos prerrequisitos. No podremos instalar SCCM si no pasamos este comprobador. Debemos tener una cuenta de dominio para instalar el servidor y otra para realizar la instalación de los clientes. Es necesario que esta última forme parte del grupo de administradores de los equipos de la red para que funcione, por esta razón será necesario que modifiquemos nuestra política de dominio. Un requisito no menor es que necesitamos una gran capacidad de disco, ya que este servidor también actuará como punto de distribución en la red. Esto quiere decir que en él se instalarán varios paquetes de instalación de parches y software de todo tipo. Si decidimos optar por instalar la base de datos de forma local, estamos hablando de 200 a 300 GB de disco para estar medianamente cómodos. Este servidor debe ser alcanzado por todos los equipos de la red; entonces, tenemos que modificar algunas reglas en los firewalls de la compañía para que los clientes puedan comunicarse y mandar información sin problemas. Dependiendo del tamaño de la empresa y su distribución geográfica, precisaremos uno o más servidores principales de SCCM. Este aspecto en particular dependerá mucho de las conexiones de red, velocidades y estructuras. Cada uno tendrá un dominio de administración y un grupo de clientes que se reportarán hacia él para brindar información de todo tipo. Sin dudas, en la instalación de SCCM se ven involucrados varios departamentos, entre los que podemos nombrar: Networking, IT e Infraestructura. Una vez implementado, afectará a toda la compañía. Por lo tanto, se requiere de una gran sincronización y comunicación interdepartamental.



WSUS (WINDOWS SERVER UPDATE SERVICES)

Esta herramienta se usaba antes de la existencia de SCCM para repartir parches en la compañía. En vez de bajar los parches directamente desde Internet, la empresa los bajaba a un servidor y los repartía en forma ordenada, realizando pruebas de implementación antes de hacer una instalación masiva. WSUS se instala debajo de SCCM, pero es este último el que se encarga de administrarlo.

Infraestructura y puntos de distribución

A continuación veremos los detalles de infraestructura necesarios para el funcionamiento de SCCM. Hay tres tipos de objetos principales en la infraestructura que debemos considerar. El primero es el servidor principal, el primero en instalarse en la red de SCCM, el que tiene la aplicación SCCM instalada. Este servidor principal se define como **site server**. Luego, están los objetos **clientes**, que se instalan en los equipos servidores, desktops y equipos móviles de la empresa. Son miniprogramas que permiten establecer la comunicación con el site server. Sin el cliente instalado, no podremos administrar el equipo. Por último, están los **Distribution Point** o **DP** (puntos de distribución), que son los servidores a donde los clientes van a buscar los parches y programas por instalar. También contienen las imágenes de sistemas operativos en caso de hacer un despliegue corporativo. Estos servidores no requieren ser exclusivos de System Center, pero sí necesitan espacio para volcar los parches y el software. El site server oficiará también de punto de distribución, ya que el rol se instala por defecto; hablaremos sobre los roles más adelante.

También el tamaño de la empresa y la geografía nos indicarán la cantidad de servidores que necesitamos tener como puntos de distribución. Habrá dos tipos de puntos de distribución: uno se llamará punto de distribución **Estándar**, y el otro, **Branch** (rama). La diferencia principal es que este último consume muchos menos recursos y puede instalarse en un sistema operativo XP. El primero debe estar instalado en sistemas operativos servidores, como Windows Server 2003 o 2008. Todos los clientes se reportarán ante el site server para mandarle información sobre el estado de cada dispositivo y, también, sobre parches, software, datos de uso, etc. El site server tendrá un rol de **Management point** (veremos los detalles en las siguientes secciones, luego de aprender a instalar SCCM).

Debemos tener muy en cuenta los anchos de banda disponibles en nuestra red, ya que por ellos transportaremos grandes cantidades de información. El traspaso de software a un equipo en particular se realiza mediante **BITS**.

La distribución de paquetes entre los puntos de distribución estándar al momento de replicarse no se realiza con BITS y esto puede consumir un poco más de recursos de la red. Todos estos elementos se agrupan para definir el site. Es posible tener un site definido en la Argentina, otro en España y otro en China, por ejemplo.



BITS (BACKGROUND INTELLIGENT TRANSFER SERVICE)

Este servicio hace que no se consuma todo el ancho de banda del cliente, porque lo limita a 256 KB. La bajada de un paquete de actualización o software es imperceptible por el usuario debido a que no hay consumo de su equipo. Puede seguir trabajando sin ningún problema en sus tareas diarias y a la velocidad normal de uso cotidiano.

Debemos tener en cuenta que cada uno dependerá de otro y se replicarán entre ellos. En este sentido es interesate recordar que existe una jerarquía entre ellos según la cual el que está más alto define reglas para los que están más abajo. Cada site maneja gran cantidad de clientes.

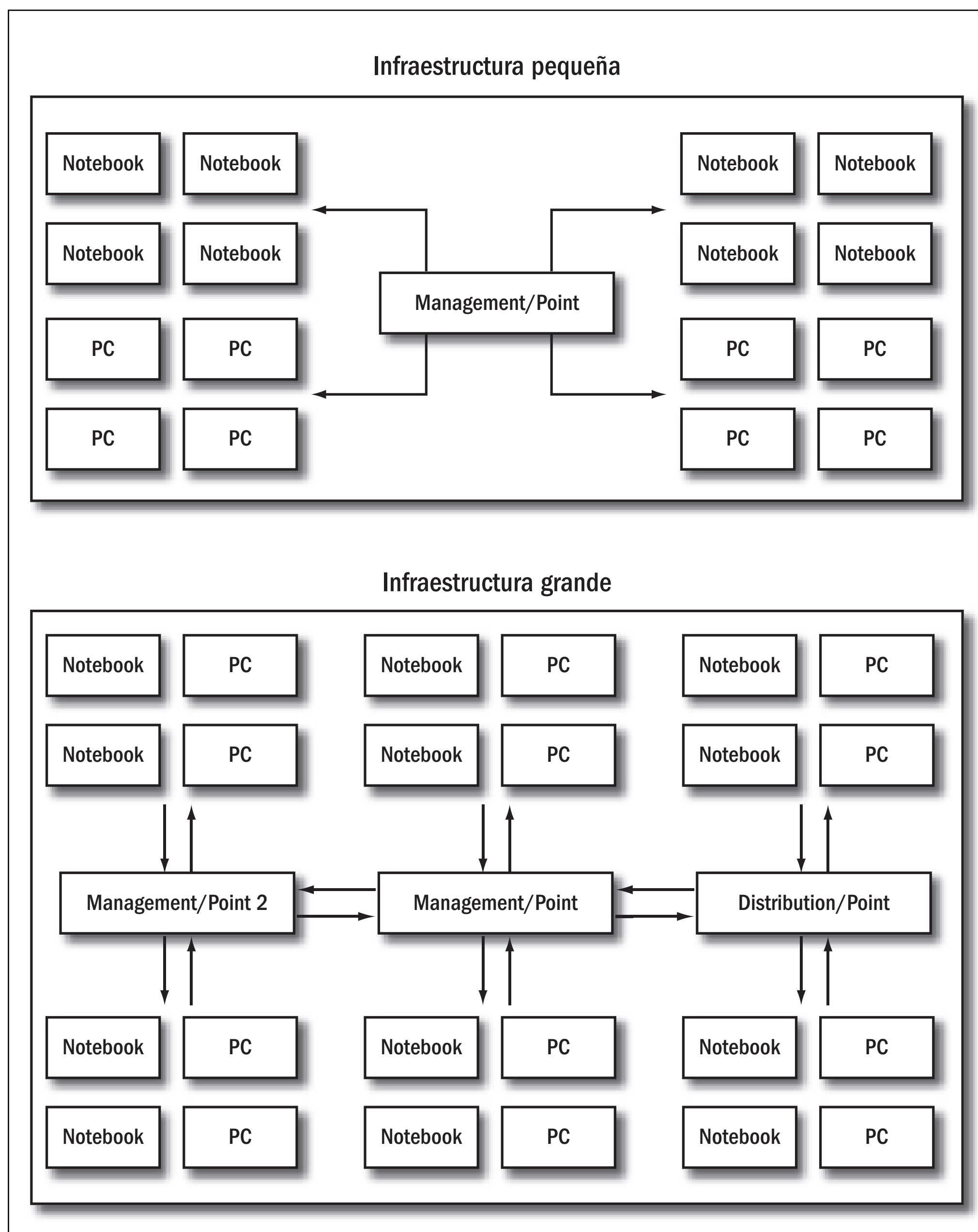


Figura 1. *Vemos en la imagen cómo la infraestructura puede ser pequeña, pero llegar a crecer.*

Instalación de SCCM

A continuación, veremos la forma correcta de realizar la instalación de SCCM. Ya pasamos lista a los prerrequisitos que necesitamos tener en cuenta; ahora debemos conocer cómo repartir los roles en la infraestructura y, también, definir cuántos sites necesitamos y cuántos puntos de distribución, entre otros elementos. Una vez completados esos pasos, procederemos a realizar la instalación de SCCM, el servidor principal, para lo cual seguimos las próximas instrucciones.

Cómo instalar SCCM — PASO A PASO

1 En primer lugar coloque el CD de instalación de la aplicación correspondiente y ejecútelo. Aparece un menú en el que puede ejecutar un analizador de prerrequisitos. Luego de esto, debajo del subtítulo denominado **Install** elija la opción **Configuration Manager 2007**.







WINS (WINDOWS INTERNET NAMING SERVICE)

Se trata de un servicio que se instala en servidores Windows, y que instala un servidor de nombres de Microsoft para NetBios. Mantiene una correspondencia entre la dirección IP y el nombre NetBios del equipo en la red. Permite no tener equipos haciendo broadcast para buscar los nombres y reduce el tráfico de red. Se ha dejado de usar para dar paso a DNS y Active Directory.

2 Se abrirá una pantalla para darle la bienvenida y le ofrecerá un resumen de las tareas por ejecutar. Oprima **Next**, elija **Install a Configuration Manager site server** y presione **Next**.



3 Para continuar, acepte la licencia marcando el casillero correspondiente y oprima la opción denominada **Next**. Posteriormnete, elija la opción **Custom settings** para realizar una instalación personalizada.



4 Elija la primera opción, el **Primary site**. Oprima **Next**, elija o no participar en el programa de experiencia del usuario de Microsoft, pulse **Next**, coloque el número de serie y presione sobre el botón llamado **Next**.

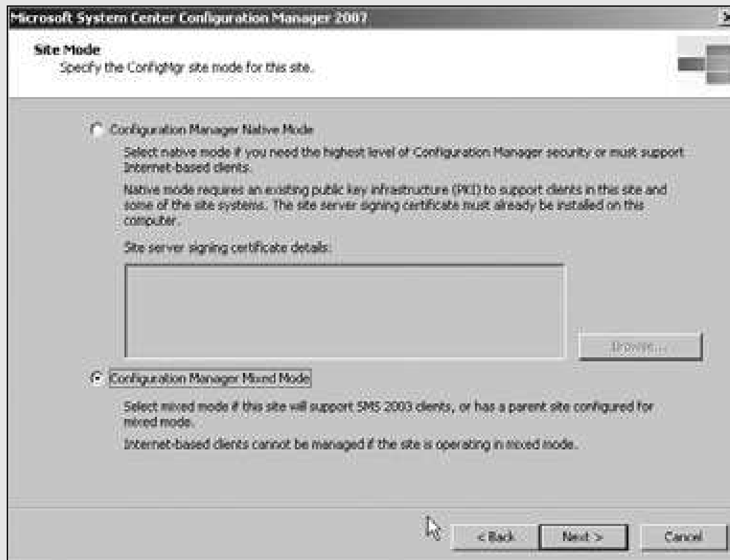


5 En este paso deberá colocar la ruta donde va a instalar el programa. Oprima el botón llamado **Next** y luego coloque un código de tres letras para el site en **Site code** y un nombre en la casilla **Site name**.



▶

6 En el paso siguiente, será necesario que elija el modo denominado **Mixed Mode**. De esta forma, será posible acceder al soporte para clientes antiguos, manteniendo la compatibilidad con ellos.

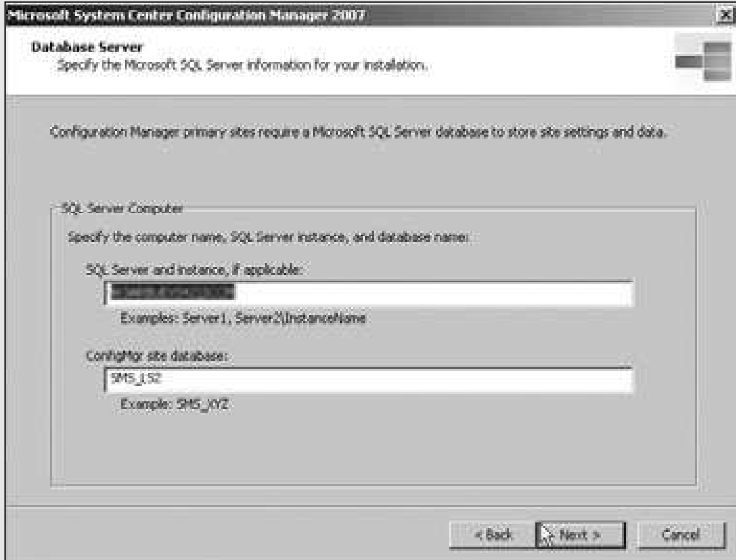


7 Posteriormnete, escoja los agentes que se van a instalar. Debe tener en cuenta que conviene dejar los que están seleccionados en forma predeterminada; de todas maneras después podrá modificarlos.

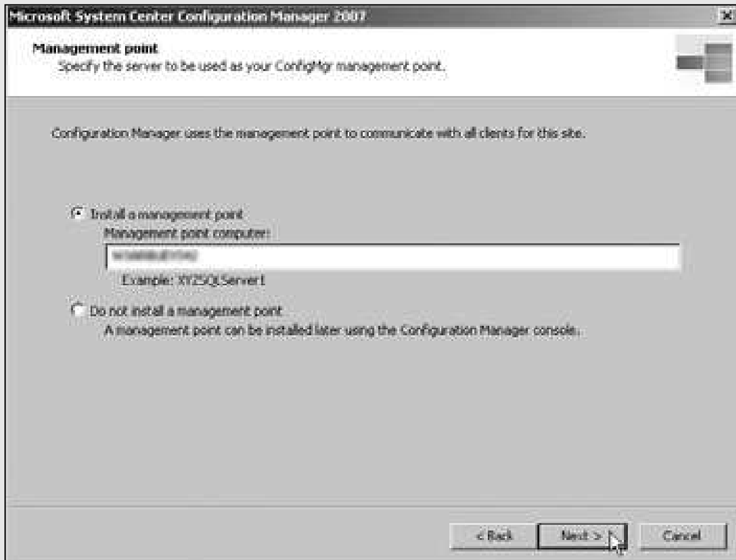


▶

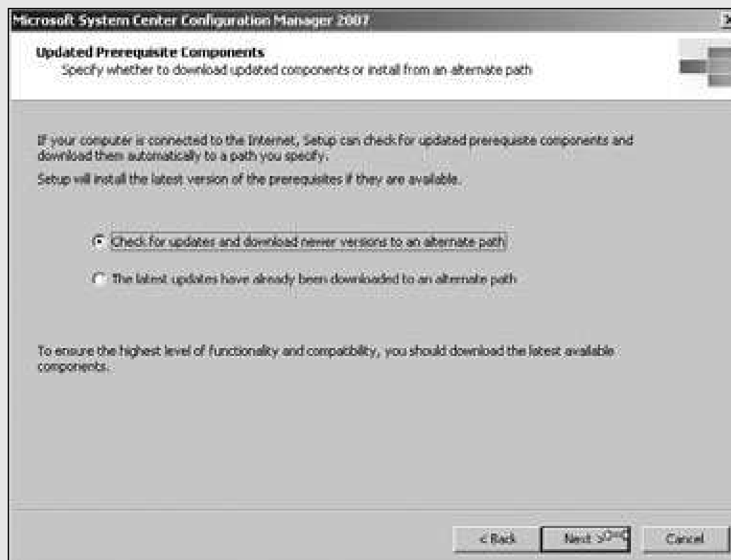
8 En la pantalla que sigue elija el servidor y la instancia de base de datos a donde conectarse. Luego, será necesario que escoja un nombre para la base de datos de SCCM. Haga clic sobre **Next** para continuar.



9 Elija el proveedor de la instalación y deje el nombre del servidor en el que está instalando la aplicación. Oprima **Next** y coloque el mismo nombre para instalar el **Management Point**.



10 Coloque un puerto HTTP para trabajar con los clientes, oprima **Next** y elija **Check for updates and download newer versions to an alternate path**, para bajar las últimas actualizaciones de prerrequisitos para los clientes.

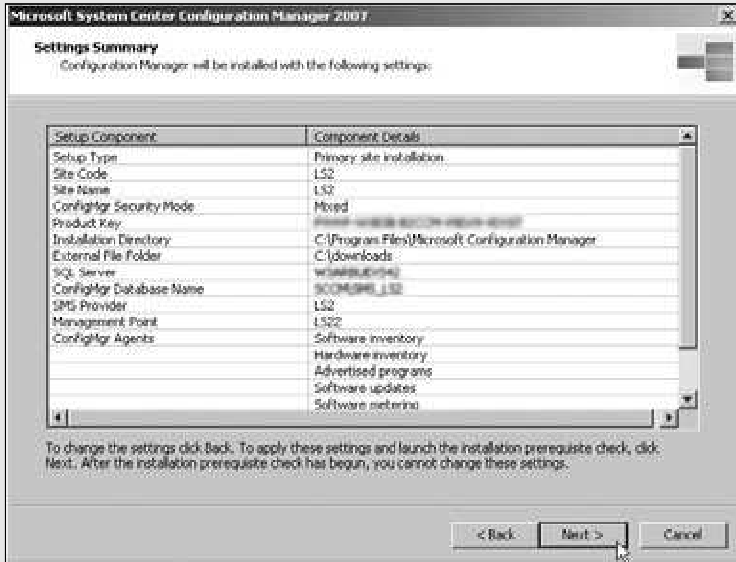


11 Seleccione la ubicación de donde bajar los parches correspondientes. Para bajarlos, será necesario que permanezca conectado a Internet. Haga clic en el botón **Next** y se iniciará la descarga.

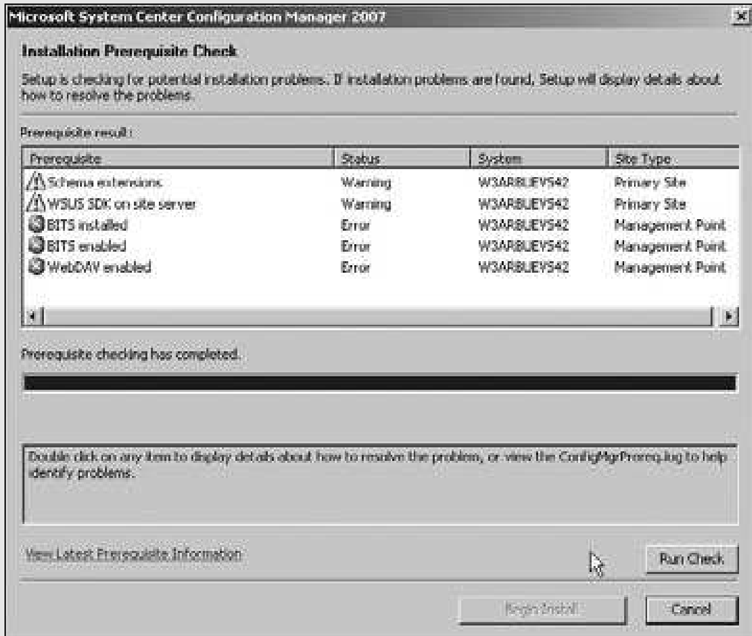


▶

12 Haga clic en **Ok** en la advertencia que muestra el fin de la actualización. Luego, vea el resumen y oprima **Next**.



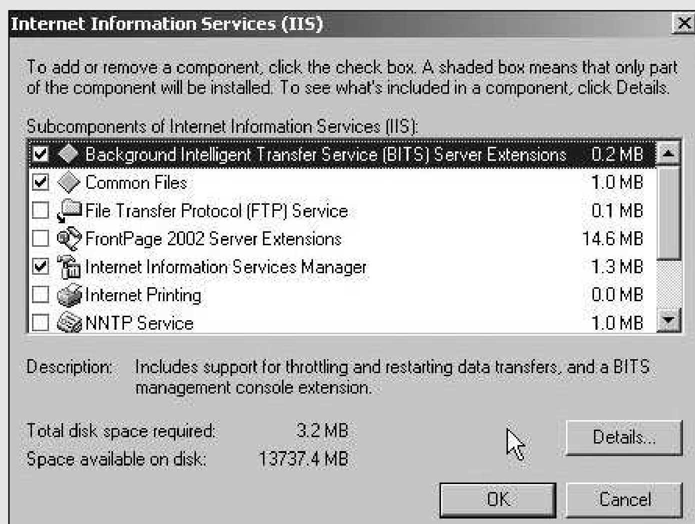
13 En esta pantalla se realizará un prechequeo de los prerrequisitos. Debe instalar y configurar lo que esté en rojo.



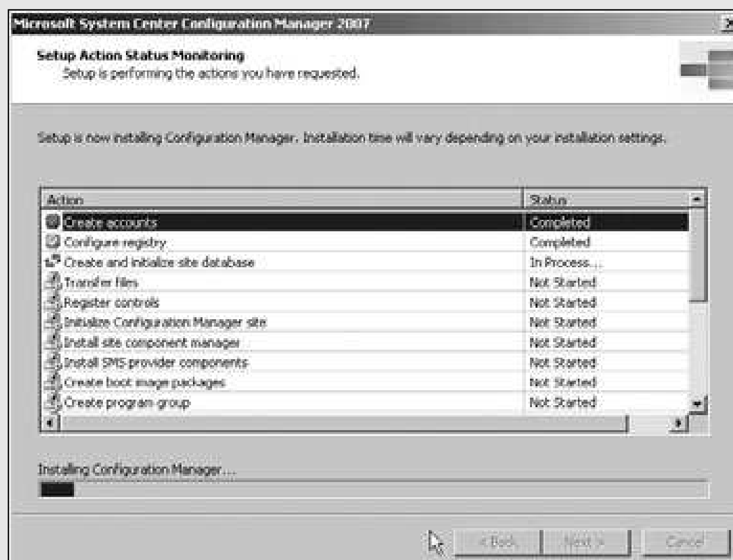
▶

▶

14 Vaya a los elementos de Windows en **Agregar o quitar programas** y, en las opciones de **Servidor de aplicaciones**, elija las opciones de **Instalar Internet Information Services (IIS)**. Seleccione **Extensiones de Servicio de transferencia inteligente en segundo plano (BITS)** y, en las opciones de **Servicio World Wide Web**, marque **Publicación en WebDav**.



15 Ejecute el prechequeo otra vez y oprima el botón **Begin Install** para comenzar con la instalación. Esto demandará varios minutos. Luego vea el resumen y oprima **Finish**.



El procedimiento que debemos seguir es sencillo, pero es fundamental prestar mucha atención y llevar documentados todos nuestros pasos mediante anotaciones a un lado, para no tener ningún problema el día de mañana si necesitamos reinstalar el sistema.

Roles de servidores

Un **rol** en SCCM es una caracterización que se le da a un servidor, una responsabilidad dentro de la infraestructura. Existen varios roles que explicaremos a continuación, pero los primeros tres son los principales que ya nombramos anteriormente. En total, son 15 roles los que tenemos para instalar:

- **Management Point (MP)**: sin dudas, es el que tendrá mayor responsabilidad. Su principal actividad es recabar información de toda la red, analizar y controlar la infraestructura. Trae y lleva información hacia y desde los clientes y servidores. Este rol puede o no estar instalado en el site server; podría instalarse en otros puntos para reunir información de los clientes de manera más balanceada y distribuida. Aunque parezca correcto pensar en distribuir esta carga, no es realmente necesario hacerlo. La información que viaja es sólo texto y podrían ocasionarse más retardos de replicación entre los MP que tengamos. Es una tarea de prueba y error para saber cuál es la mejor opción en nuestra red.
- **Distribution Point (DP)**: este rol se ocupa, básicamente, de distribuir parches y programas a toda la compañía. Se genera un repositorio de parches al cual pueden acceder todos los equipos, y es allí donde los clientes van a buscar los paquetes de parches y programas.
- **Site Server**: se trata de una opción que nos informa que pertenece al servidor principal, es el que define un sitio principal de SCCM.
- **Site System**: al igual que Site Server, es un rol exclusivo del servidor principal.
- **Component Server**: indica que existe un servidor de componentes. Es un rol que se instala en cada servidor que cumpla un rol. Tendremos un Component Server en el MP, y otro elemento similar si instalamos otro rol en otro servidor.
- **Fallback Status Point**: indica los estados de fallos. Se utiliza para recibir información de clientes que no se han podido instalar, de aquellos que no se pueden contactar, y otros tipos de fallas. No se instala por defecto. Es recomendable si tenemos muchos problemas con la instalación de los clientes.
- **Reporting Point (RP)**: se lo usa para crear un website de reportes; sólo es necesario uno por site. Podemos darnos cuenta de que trae muchos reportes predefinidos y también podremos crear los nuestros.
- **Server Locator Point (SLP)**: se encarga de informar a los futuros clientes de SCCM cuál es su MP asignado para que instalen el software cliente.
- **Software Update Point (SUP)**: esta opción se encarga de indicarnos que ya existe un distribuidor de parches instalado y funcionando.

- **Site Database Server**: indica el servidor que contiene el MSSQL funcionando.
- **Reporting Service Point (RSP)**: con este rol y las funciones de Reporting Services de MSSQL, podemos instalar un servidor de reportes más potente, aprovechando todas las ventajas de reporting, com informes programados y preconfigurados.
- **System Health Validator Point (SHVP)**: es muy particular, ya que debe estar instalado sólo en servidores que tengan que utilizar NAP (*Network Access Protection*).
- **State Migration Point (SMP)**: es el encargado de recabar información de los usuarios y hacer un backup hasta que su computadora sea migrada o reinstalada mediante la distribución de sistemas operativos de SCCM.
- **PXE Service Point (PXE)**: se necesita en ambiente de distribución de sistemas operativos, exclusivamente.
- **Out of band Service Point (OSP)**: se utiliza para manejar equipos que se encuentran fuera del dominio, en otra red.

Luego de analizar los distintos roles que puede tener un servidor en la infraestructura de SCCM, realizaremos un procedimiento para aprender a instalar cualquier rol en cualquier servidor. Todos estos roles pueden instalarse por completo en el Site Server o repartirse en varios servidores, según el tamaño de la infraestructura.

■ Cómo instalar un rol en un servidor desde SCCM — PASO A PASO

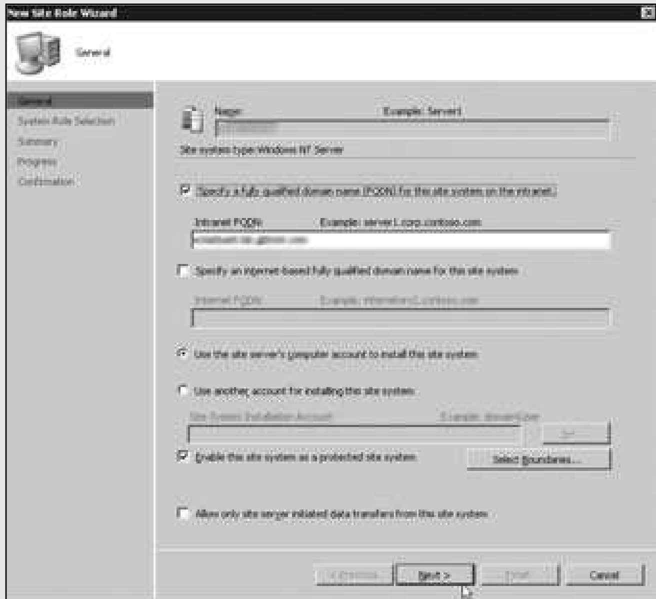
1 Vaya hasta la consola de SCCM y elija unos de los servidores en **Site Systems**. Haga clic derecho arriba y seleccione **New Roles** para instalar un nuevo rol en el servidor objetivo; o haga clic con el botón derecho del mouse sobre **Site Systems** para instalar un nuevo servidor con un nuevo rol.



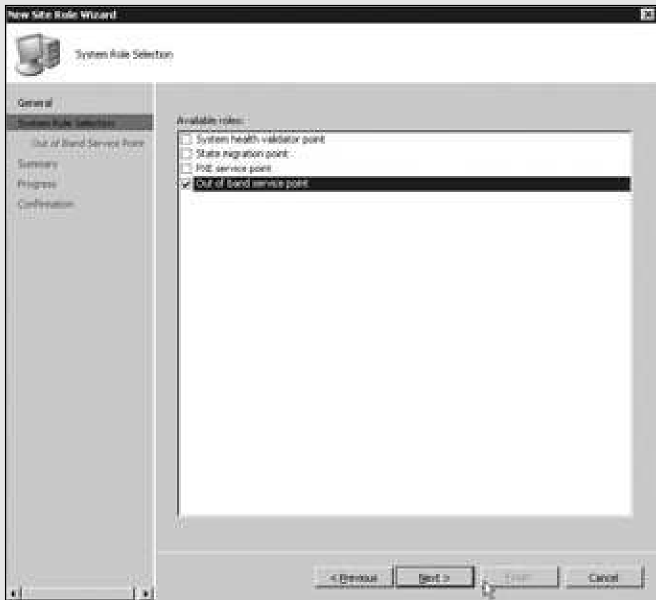
▶

▶

2 Ingrese el nombre completo del servidor en **Intranet FQDN**, deje las configuraciones como están y oprima **Next**.



3 En este paso elija el rol que quiere instalar. Figurarán los que no haya instalado previamente. Coloque la marca correspondiente y oprima **Next**.



▶

▶

4 Seleccione las opciones que más le agraden. Esta pantalla variará según el rol que haya querido instalar. Se recomienda leer la documentación previamente.

5 Vea el resumen de las tareas por realizar, oprima **Next** y, luego que las tareas se realicen, oprima **Close**.

CLIENTES DE SCCM

Ya vimos los prerrequisitos y la instalación concreta de SCCM. Una etapa muy interesante es la instalación de los clientes, porque sin ellos, SCCM no funcionaría. Hay muchos errores posibles y algunas formas de solucionarlos, pero es una tarea cotidiana verificar que todos funcionen correctamente. A continuación, veremos los detalles de instalación y las formas de corrección.

Características de los clientes

Los clientes de SCCM son software que debe instalarse en las computadoras de escritorio, servidores y dispositivos móviles para que éstos puedan ser administrados por SCCM. Son un puente de comunicación entre el servidor y el cliente final, y son necesarios para que la máquina comience a reportar su estado, su inventario, el uso de los programas, etc. Sin él, es como si quisiéramos llamar a alguien que no tiene teléfono: jamás lograríamos comunicarnos. Más adelante veremos las formas de instalación, pero generalmente el cliente de SCCM se instala en la carpeta **c:\Windows\system32\CCM**, y la carpeta de instalación estará en **c:\Windows\system32\ccmsetup**. En sistemas de 64 bits veremos que la misma carpeta del cliente está en **C:\Windows\SysWOW64\CCM** y la de instalación, en **C:\Windows\ccmsetup**. Debemos tener en cuenta estas pequeñas diferencias en los nombres. En la carpeta del cliente tendremos también todo tipo de **logs**, archivos DLL y más archivos de la aplicación. Hay una carpeta que necesitaremos conocer cuando la instalación de un parche falle. Es la **caché**, en la cual se bajan los archivos de actualizaciones por instalar.

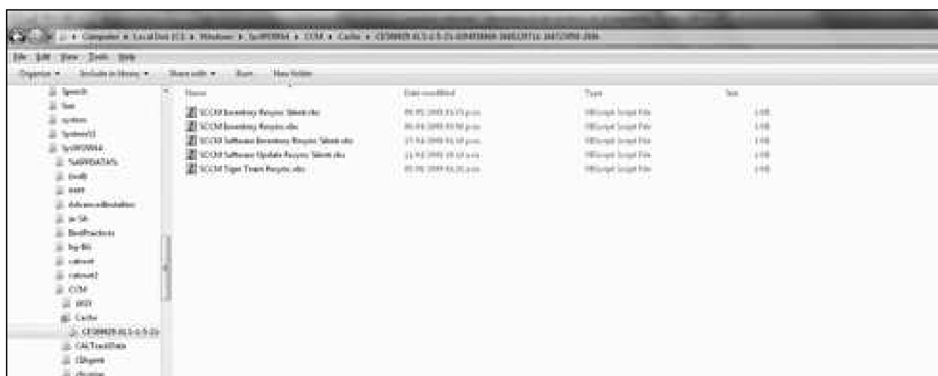


Figura 2. *Vemos un paquete dentro de la carpeta caché. Podemos tener varios paquetes, que son los instaladores de nuestros parches y software.*

En caso de falla, debemos borrar el contenido y volver a sincronizar contra el servidor MP. Luego de instalarse el cliente, veremos algunos iconos nuevos en el **Panel de control**, que corresponden a cuatro aplicaciones:

- Configuration Manager (administrador de configuración)
- Program Download Monitor (monitor de bajada de programas)
- Remote Control (control remoto)
- Run Advertised Programs (correr advertencias de programas)

Configuration Manager tiene varias solapas. Nos informa todos los datos de nuestro equipo, entre ellos, el site al cual pertenece el cliente, la versión del cliente, el tipo de conexión contra el servidor, los detalles de red y del usuario, el MP al cual pertenecemos, nuestro sistema operativo y el modo en el que está trabajando el site. También tendremos la información sobre el estado de todos los componentes del sistema y un listado de acciones que podemos llevar a cabo. Hay también una solapa de opciones avanzadas, en la cual podemos definir el site a donde pertenece ese cliente y el lugar donde se instalarán los parches. **Run Advertised Programs** nos permite ejecutar aplicaciones disponibles en el servidor para ser instaladas.

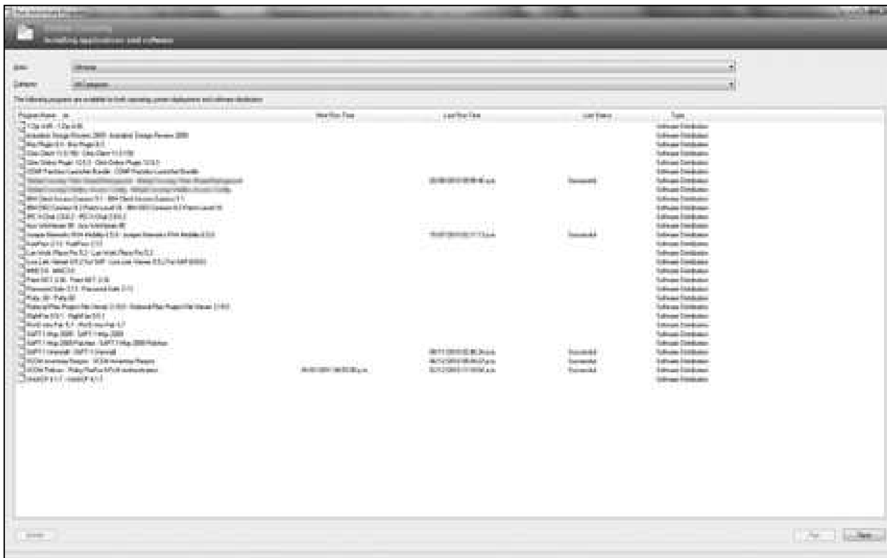


Figura 3. *Aquí se muestra un listado, y nosotros elegimos cuál instalar. Se abre una ventana de bajada que nos indica el progreso.*



DLL (DYNAMIC LINK LIBRARY)

Son archivos con código ejecutable, cargados por el sistema operativo bajo demanda de un programa en ejecución. Se utilizan para no sobrecargar la memoria, y se usan sólo los que se necesitan. Cada DLL puede estar compartida por varios programas, y debemos tener cuidado en sus actualizaciones, porque podemos afectar a varios de ellos.

Si abrimos el **Program Download Monitor**, también veremos el progreso. Éste es el encargado de decirnos que tenemos nuevos programas disponibles para instalar, mediante un icono en la barra de tareas. Por último, el programa **Remote Control** se utiliza para que alguien nos asista desde fuera de nuestra máquina.

Prerrequisitos de instalación

Es importante mencionar que unos de los puntos importantes antes de la instalación es el modo de publicación del site para saber cómo vamos a contactarlo. También debemos pensar si el cliente pertenece o no al dominio en donde está el site: puede ser que el site esté en un dominio y el cliente, en otro. Debe haber una relación de confianza entre dominios donde poder tener los mínimos privilegios para acceder a la máquina destino. Los clientes no podrán encontrar el site vía DNS, sino que lo harán por WINS. Más adelante, en este mismo libro, veremos la forma en que podemos revisar los servicios necesarios en el futuro cliente.
Los futuros clientes deben tener instalada y configurada la opción denominada **Compartir archivos e impresoras**. Nuestros firewalls tienen que estar configurados para dejar comunicarse a los clientes y a los servidores. Es necesario que tengan habilitados los puertos 80 y 443 para la comunicación con el site. De la misma forma, para que tengan comunicación con el SHVP, precisamos habilitar los puertos 67 y 68 del protocolo UDP, y el 80 y el 443 para IPsec; el 2701, 2702 y 135 del protocolo TCP serán para utilizar el servicio de Remote Control. Una vez que contemos con esos puertos abiertos, ya podemos pensar en instalar el cliente. En resumen, podemos listar los siguientes puertos:

- **80 (TCP) (IPsec)**
- **443 (TCP) (IPsec)**
- **67 (UDP)**
- **68 (UDP)**
- **2701 (TCP)**
- **2702 (TCP)**
- **135 (TCP)**



WMI (WINDOWS MANAGEMENT INSTRUMENTATION)

Microsoft implementa WBEM mediante este servicio. Se trata de una iniciativa para establecer normas estándar que permitan tener acceso y compartir información a través de la red para la administración de los equipos. También proporciona compatibilidad con CIM (**Common Information Model**), que permite describir los objetos existentes en un entorno de administración.

■ Verificar prerrequisitos para instalar un cliente PASO A PASO

1 Entre en la consola de servicios del futuro cliente. Revise si tiene el servicio de Windows **Adaptador de rendimiento WMI** (WMI), también conocido como **WmiApSrv**, en modo automático y en ejecución.



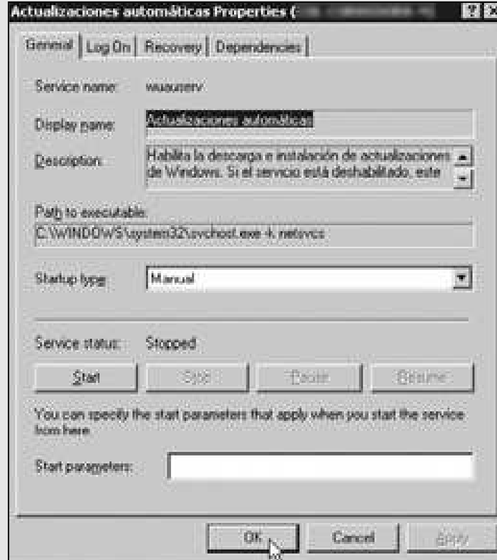
2 Verifique que el servicio llamado **Servicio de transferencia en segundo plano** (**BITS**) esté en modo automático y en ejecución.



►

▶

3 Para continuar, cambie el servicio denominado **Actualizaciones automáticas**, también conocido como **wuauserv**, al modo **Manual**, y posteriormente detenga su ejecución con el botón correspondiente.



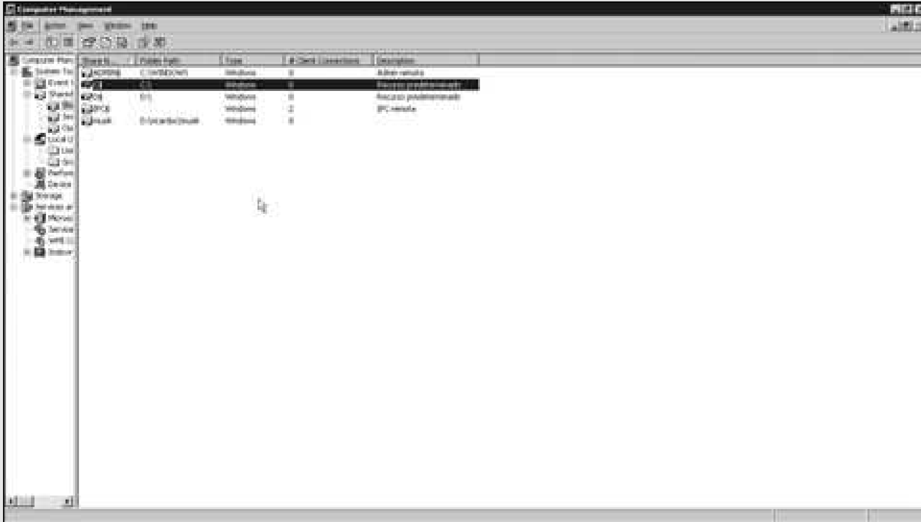
4 Luego deberá controlar que el servicio **Registro Remoto** esté también en modo automático y ejecutándose. Para realizar esta tarea acceda a las propiedades que corresponden al servicio y presione las opciones adecuadas.



▶

▶

5 En los recursos compartidos, verifique que el futuro cliente tenga los directorios de administración compartidos, el **c$** y el **ADMIN$** con los permisos suficientes para que ingresen los administradores.

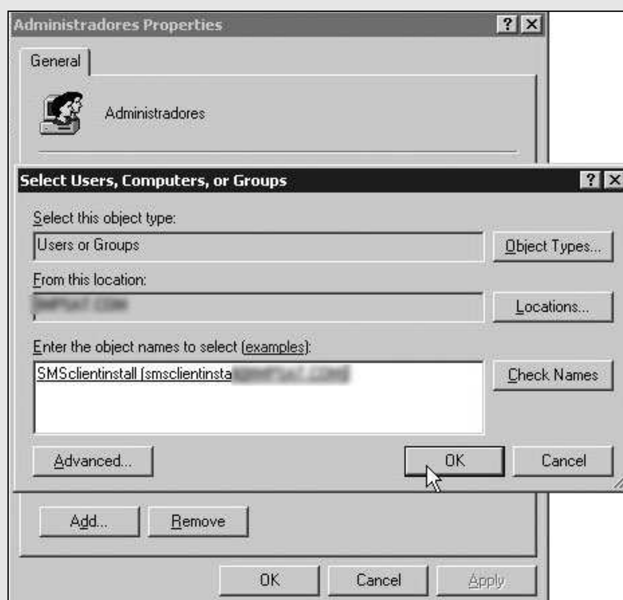


6 En la administración del sistema, vaya hasta el controlador llamado **WMI**, haga clic derecho con el mouse sobre él y elija las propiedades. Se abrirá una ventana similar a la que muestra la imagen siguiente.



▶

▶ **7** Por último, verifique que el cliente de administración de SCCM pertenezca al grupo **Administradores** de los grupos locales del equipo que pretende instalar.



Todos estos prerrequisitos y chequeos pueden verificarse creando una o varias políticas de seguridad para el dominio. De esta forma, nos aseguramos de que todas las PCs cumplan con lo requerido para que SCCM se instale de forma remota.

Instalación de clientes y sus problemas

Tenemos varias formas posibles de realizar la instalación de los clientes de SCCM:

- Automática, desde la consola de SCCM
- Push, también desde la consola SCCM
- Vía GPO, desde el Active Directory
- Manual, con un programa **ccmsetup**, que viene en la instalación de SCCM. Hay dos opciones: la ejecutable .EXE y la autoinstalable .MSI.

Sin dudas, la mejor forma es la **Automática**, porque permite que se autoinstalen los equipos recién descubiertos por la herramienta. Tiene un motor de instalación que va controlando su progreso e informa el motivo de la falla en caso de ocurrencia. Para que funcione correctamente, hay que configurar bien sus opciones. A continuación, veremos cómo hacerlo. Las opciones del MSI son varias:

OPCIONES MSI	DESCRIPCIÓN
SMSSITECODE	Especifica el site al cual debe estar dirigido el cliente. Siempre se conforma por nombres de tres letras. Se podría poner la opción AUTO también para que el site se asigne vía Active Directory o Locator Point.
SMSMP	Debemos indicar el servidor que oficiará como Management Point de este cliente.
FSP	Le dice al instalador dónde se encuentra el servidor con el rol de Fallback Status, para que pueda informar sus errores.
SMSSLP	Indica dónde se encuentra el Server Locator Point, será el Management Point.
RESETKEYINFORMATION	Se utiliza en caso de que ya haya habido un cliente instalado y se haya cambiado de Management Point. Si el cliente perdió conexión, no se le pudo informar y quedó mal configurado. En ese caso, con esta opción se resetea y se le vuelve a configurar el indicado.

Tabla 2. *Opciones de MSI para la instalación del cliente ccmsetup.msi.*

Un buen ejemplo, una buena línea de instalación completa sería la siguiente:

```
SMSMP=w3arbue5.lat.gblxint.com SMSSITECODE=LS1 FSP=w3arbue5.lat.gblxint.com
SMSSLP=w3arbue5.lat.gblxint.com RESETKEYINFORMATION=TRUE
```

El método **Push** es similar y utiliza las mismas opciones. El motor de instalación genera un log importante que ayudará a controlar los problemas. El log se encuentra en: **C:\Archivos de Programas\MicrosoftConfiguration Manager\Logs\ccm.log**. Podemos instalar la herramienta **ConfigMgr 2007 Toolkit**, que incluye una en especial denominada **SMS trace**, y nos permite abrir un archivo log y analizarlo mientras se continúa escribiendo, y ver las actualizaciones a medida que se escriben.



Figura 4. *Podemos observar la herramienta SMS Trace analizando uno de los logs de un cliente SCCM.*

La instalación por GPO es sencilla, pero no tendremos control de lo que sucede con la instalación, como desde la consola. Debemos armar una política de instalación de software con el archivo que se encuentra en el CD de instalación del SCCM, en:

SMSSETUP\BIN\I386\CCMSETUP.MSI. También podemos importar del CD de instalación en la ubicación: **\TOOLS\ConfigMgrADMTemplates**. La última forma de instalación que revisaremos es la manual. Implica copiar la carpeta de instalación del cliente y, por línea de comandos, ir hasta el ejecutable: **Ccmsetup.exe +opciones**.
Las opciones de instalación de ccmsetup.exe son muy variadas, hay 44 en total. Deben estar bien configuradas y probadas para no incurrir en errores masivos. Tenemos varias opciones, que se resumen en la **Tabla 3**; sólo distinguiremos las más importantes.

OPCIONES DE CCMSETUP.EXE	DESCRIPCIÓN
/source:<ruta>	Especifica la localización de los archivos de instalación del cliente.
/mp:<Management Point>	Debemos indicar el servidor que oficiará como Management Point de este cliente.
/service	Especifica que el programa de instalación debe ejecutarse como servicio con la cuenta del sistema.
/forcereboot	Le dice al programa que reinicie el equipo si es necesario para completar la instalación.

Tabla 3. *Opciones del instalador ccmsetup.exe.*

Veremos a continuación un paso a paso que nos indicará qué necesitamos tener en cuenta en cada modo de instalación para los clientes.

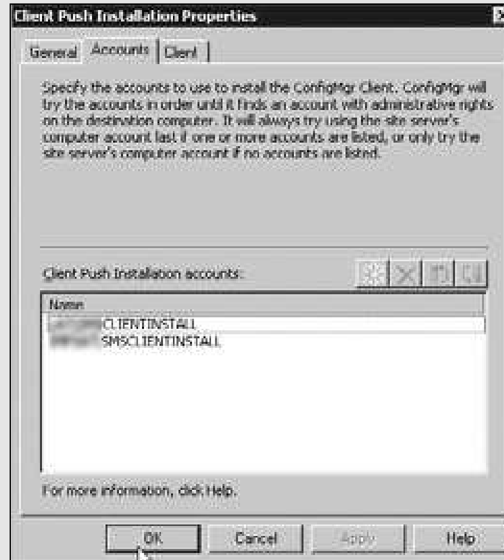
■ Cómo instalar un cliente SCCM — PASO A PASO

1 Para la instalación automática, vaya en la consola de **SCCM** hasta **Site Settings/Client Installation Methods**. Allí haga un clic derecho en **Client Push Installation**. En **General** marque **Enable Client Push Installation to assigned resources.** Seleccione los tres roles para instalar y para los sistemas sites.

►

▶

2 En la solapa denominada **Accounts** deberá colocar las cuentas que tienen permisos de administración del dominio en todos los equipos correspondientes. Recuerde que puede incluir una o varias cuentas.



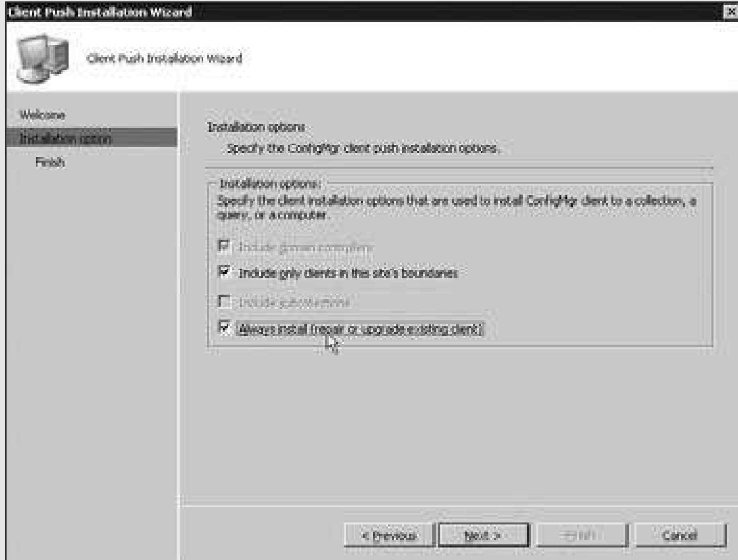
3 Para continuar, deberá tener en cuenta la necesidad de colocar los parámetros MSI apropiados para sus clientes debajo de la sección llamada **Installation Properties**, en la solapa **Client**.



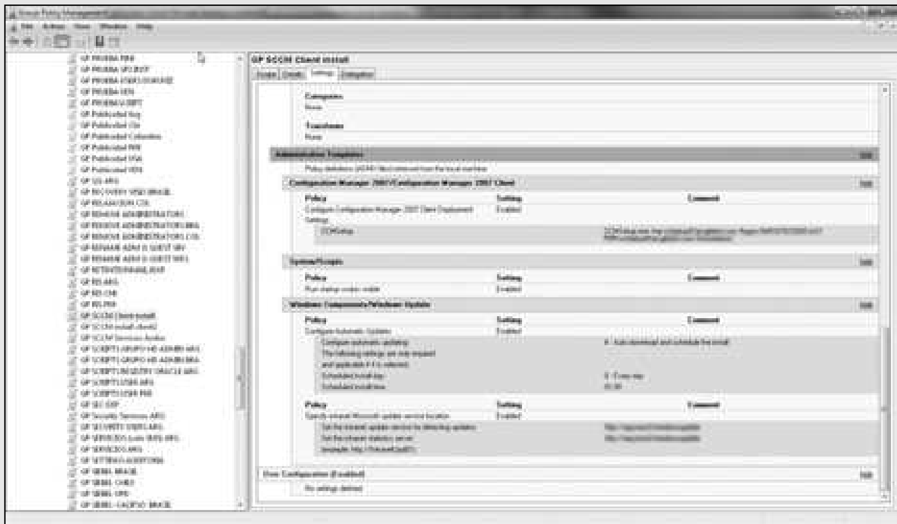
▶

▶

4 Para el método **Push** (manual), necesita ir hasta el objeto del dispositivo objetivo y hacer clic derecho; luego elija **Install Client**. Se abrirá una breve ayuda; marque todas las opciones posibles, oprima **Next** y, luego de ver el resumen, pulse **Finish**.



5 Para utilizar la política, debe importarla desde el CD de instalación. Luego edítela y modifique los parámetros de **CCMSetup**, **Configure Automatic Updates** y de la opción **Specify Intranet Microsoft update service location**. Asígnela a la OU correspondiente donde estén los futuros clientes.



▶

6 Por último, en la línea de comandos, vaya hasta la carpeta **c:\Windows\ccmsetup** y ejecute **ccmsetup.exe** con los parámetros adecuados para sus clientes.

Todas estas opciones son válidas y pueden usarse en conjunto, pero si funciona la instalación automática, todas las demás no son necesarias. Para desinstalar un cliente, debemos ejecutar el comando **ccmsetup.exe/uninstall**.

Formas de descubrir clientes

Cuando hablamos de descubrir clientes, nos referimos a la manera en que SCCM encuentra nuevos equipos que administrar en nuestra red. Por supuesto, no tendremos que agregar uno por uno manualmente. En **Site Management/Nombre del Site/Site Settings Discovery Methods** estarán todas las opciones de descubrimiento y podremos configurarlas a nuestro gusto, así como habilitarlas o deshabilitarlas. Contamos con seis posibilidades de descubrir nuevos clientes:

- Active Directory System Group Discovery
- Active Directory Security Group Discovery
- Active Directory System Discovery

- Active Directory User Discovery
- Heartbeat Discovery
- Network Discovery

Todas estas opciones nos permiten tener nuevas máquinas a las cuales instalar el cliente de SCCM. Cada una busca de distinta manera información sobre clientes y nuevos futuros clientes. Iremos nombrándolas en orden de importancia. La primera, y más importante, es **Active Directory System Discovery**. Este servicio busca nuevas máquinas que no estén en la consola de SCCM, en lugares específicos del AD. Podemos colocar una consulta LDAP o elegir algún sitio particular dentro del directorio, alguna OU determinada o distintos dominios. Cuando hablamos de consulta LDAP, nos referimos a una consulta al controlador de dominio. LDAP es el lenguaje que entiende su base de datos. Una consulta LDAP nos indica un lugar en el directorio o una propiedad particular de cualquiera de sus objetos. Se usa regularmente en la administración de Active Directory.
Otro importante descubridor de objetos es **Active Directory User Discovery**. Es similar al anterior, pero descubre usuarios de una ubicación específica del AD. El siguiente es **Active Directory Security Group Discovery**, que también busca en ubicaciones específicas del AD, pero rastrea grupos de seguridad, locales, globales y universales. El siguiente tipo, **Active Directory System Group Discovery**, no es precisamente para buscar nuevos clientes, sino que busca información en el AD de clientes que ya están instalados. Busca información adicional, como puede ser sobre la OU en la que se encuentra el cliente, a qué grupos pertenece y qué usuarios tienen acceso. **Heartbeat Discovery** es utilizado por SCCM para actualizar sus clientes descubiertos en la base de datos. Esta opción la manda a correr un cliente con modo activo y no se ocupa de descubrir nuevos clientes. Por último, el menos utilizado es **Network Discovery**, que busca por toda la red dispositivos que tengan una IP. Puede ser útil para descubrir otro tipo de objetos en la red, como impresoras, routers, etc. Como SCCM no puede hacer mucho con este tipo de elementos, se recomienda desactivarlo para no tener basura dando vueltas por nuestra base de datos de SCCM. Todas estas opciones de descubrimiento, menos la de Heartbeat, son tareas en la consola de SCCM, y tenemos la posibilidad de ejecutarlas cuanto antes. Es importante para el descubrimiento de máquinas que se tenga en cuenta el nombre con el cual se crea. Puede ocurrir que en el Helpdesk se utilice una imagen de un equipo para instalar todas las máquinas nuevas que se vayan creando. Luego de configurar todo, le cambian el nombre final que debería llevar. Pero es importante que lo hagan en una fase mucho más temprana, para no tener **clientes huérfanos**. Esto se da porque los métodos de descubrimiento pueden informarlo cuando se conecte o cuando se le asigne un dominio. El descubrimiento ocurre de nuevo y habrá dos nombre de clientes que corresponden a la misma máquina (uno estará activo y el otro no), pero esto se limpia después de unos días.

Consola de comprobación de clientes

Podemos ver desde la consola aquellas máquinas que no tengan clientes; aparecerá el nombre del equipo, y en la columna de cliente dirá **No**. Para volver a instalar el cliente o corregir errores, se puede hacer una instalación mediante el método push, muy rápidamente. Hay otra forma de corregir errores, y es con una consola **HTA** llamada **Client Troubleshooter**. La aplicación HTA para SCCM puede descargarse desde **www.sccm-tools.com/tools/standalone/standalone-clienttroubleshooter.html**.
La consola es un gran conjunto de comandos vbscript que ejecutan consultas por WMI para traer información del cliente. En un principio, si el servicio de WMI no está funcionando en el cliente, esta información no podrá recabarse. Como SCCM necesita WMI para funcionar, podremos descubrir rápidamente una de las causas del porqué no se instala correctamente el cliente.

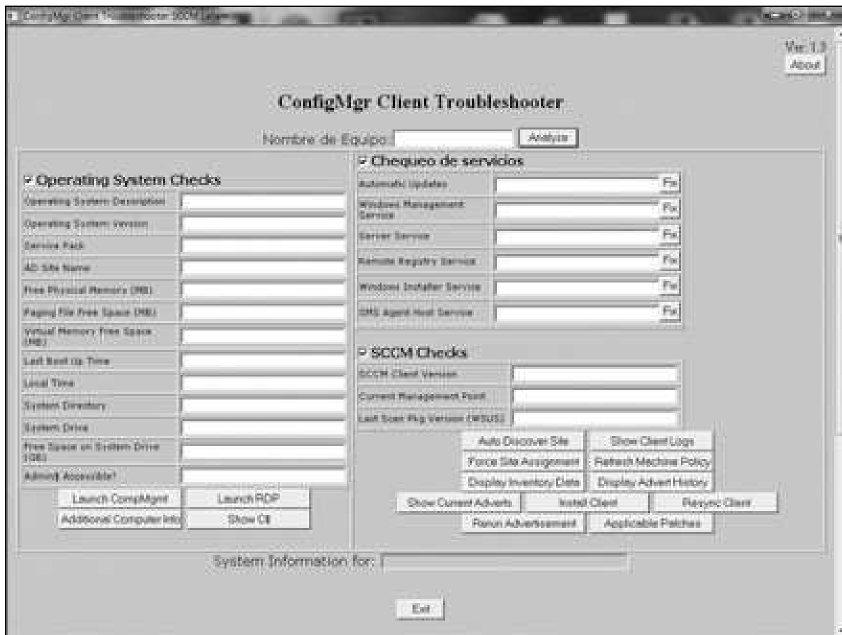


Figura 5. *Vemos en la imagen la herramienta Troubleshooter funcionando, modificada con algunas opciones de acción más.*

La información que chequea la herramienta puede agruparse en tres elementos: **chequeos de sistema operativo**, **chequeos de servicios** y **chequeos del cliente de SCCM**. Entre los del sistema operativo obtendremos información del espacio en disco, para saber si alcanza para la instalación del cliente. También la versión del sistema operativo, el último service pack instalado, datos de la memoria RAM y algo muy importante, que es el acceso al disco C. Controla los servicios que deben tener funcionando para instalar SCCM. Con respecto al cliente, se chequea su versión, el MP al cual pertenece y la fecha del último scan de parches. Entre las acciones que

podemos hacer en forma remota se encuentran: instalación del cliente, asignación de un site, refrescar la política de la máquina, correr nuevamente alguna advertencia de software o ver los parches que se pueden aplicar. También podríamos ver los logs del cliente y su inventario, abrir la administración del cliente, conectarnos mediante escritorio remoto, ver alguna información adicional y abrir el disco **C:** en caso de que necesitemos hacer espacio. En la misma herramienta, pero más abajo, encontramos una zona para realizar las tareas masivamente. Hay un recuadro en blanco para ingresar los nombres de los equipos, y botones con acciones similares a los que figuran más arriba para un solo equipo. Podemos efectuar las tareas previamente vistas a varios clientes al mismo tiempo. Sólo colocamos un listado de equipos pegando sus nombres en el recuadro que está en blanco. Luego, realizamos las acciones para todos los dispositivos al mismo tiempo. Esto acelera la reparación, ya que podríamos hacer un análisis desde la consola, exportar la lista a una planilla de cálculo y comenzar a arreglar los clientes fallidos, pero todos juntos.

La única desventaja de utilizar estos comandos batch es que no tendremos control de errores. Sólo debemos esperar y luego analizar uno por uno para ver si se reparó. Debemos adaptar la herramienta a nuestro dominio y a la ubicación de los archivos. También es posible modificarla y expandirla, agregando nuevas funciones que necesitemos. Para hacerlo, editamos el código HTML de la aplicación teniendo los conocimientos mínimos de VbScript. La ejecutamos y, en la ventana de la aplicación, hacemos clic derecho y elegimos **Ver fuente**. Luego, cambiamos las siguientes líneas:

```
Const strCCMSetupSource= “\\MYSCCMServer\sccmclient”
```

En esta línea modificamos la ruta donde se encuentra nuestro instalador. Podríamos ubicarlo en el netlogon, para así tener un fácil acceso desde cualquier ubicación.

```
Const strClientVersion = “4.00.5931.0001”
```

Ésta es la versión que chequeará como correcta; en caso de no corresponder, se marcará la versión en rojo.

```
Sub InstallSMS
```

Debemos tener en cuenta que es necesario modificar este procedimiento para agregar las opciones avanzadas de instalación que quisiéramos.

Para sistemas operativos Windows 7 o Windows 2008, necesitamos correr la aplicación desde una línea de comandos abierta con privilegios de administrador.

PUNTOS DE DISTRIBUCIÓN

Los **puntos de distribución** son uno de los elementos más importantes de la infraestructura. Cada uno tiene su complejidad y, en este caso, una mala arquitectura de puntos de distribución puede hacer caer nuestra red empresarial. Ya definimos qué son, por lo que ahora veremos algunos detalles sobre su instalación, la diferencia entre puntos estándar o branch, y algunas mejoras que se plantearon utilizando una red P2P y el protocolo Bittorent.

Qué tener en cuenta antes de instalar el rol DP

La instalación de puntos de distribución en una infraestructura juega un papel primordial en todo el funcionamiento del SCCM, y dependerá muchísimo del tamaño de la empresa. Si tenemos unas 40 máquinas y servidores en una sola ubicación, no habrá ningún problema; sólo deberemos instalar el rol en el servidor principal, y listo. Los 40 clientes irán a buscar parches y software al mismo servidor. La situación comienza a complicarse un poco más si tenemos esos 40 equipos distribuidos en ocho lugares diferentes. Si hubiese una conexión pobre, empezaríamos a analizar ciertos problemas que no se repetirán de la misma forma, sino que serán totalmente al azar y sin ningún patrón en común. Ahora, supongamos que tenemos tres países conectados con 840 clientes. Si éstos fuesen Argentina, Chile y Brasil, con una buena conexión, no haría falta más que un único servidor, porque las distancias son cortas. Pero si la conexión contra Brasil es pobre o en Brasil reside el 50% de los clientes de SCCM, tendríamos que pensar en instalar un punto de distribución allí. Esto descentralizará bastante la distribución de parches y la agilizará. Además, es más rápido distribuir parches en Brasil teniendo un punto de distribución allí mismo. Supongamos ahora que tenemos una sede en Ecuador y otra muy importante en Colombia, siempre con la principal en Argentina. Resulta que Ecuador no está conectado directamente contra Argentina, sino que lo está a Colombia; o sea, que los clientes de Ecuador deben pasar por Colombia antes de ir a brindar su información e interactuar con el Management Point en Argentina. Si la red entre Ecuador y Colombia posee un ancho de banda bajo, tal vez sea un cuello de botella bastante particular.



PROCESOS BATCH

Los procesos batch son secuencias encadenadas de instrucciones que se realizan una tras otra. Este grupo de tareas se efectúan a un solo objeto o a un grupo, según lo establezcamos en el proceso. Se codifican con un editor de texto y se guardan con una extensión .BAT en vez de .TXT. Las acciones masivas de la consola HTA son procesos batch.

En este caso, si distribuyéramos un software un tanto pesado, de unos 150 MB, por ejemplo, la red podría colapsar. La cantidad de máquinas yendo a buscar el paquete de instalación contra el servidor en Argentina, por más que se utilice BITS, haría caer la red, y no nos daríamos cuenta de lo que pasó hasta que apagáramos SCCM. Todos los clientes estarían conectados bajando software contra la misma ubicación, y esto saturaría el punto de distribución. Si el software fuese pequeño, los clientes lo bajarían y se desconectarían, para dejar su lugar a otro. Entonces, la solución correcta sería instalar un punto de distribución en Ecuador. Los paquetes de software y parches se replican entre los puntos de distribución. La copia de estos archivos entre los dos servidores se realiza sin usar BITS y es mucho más rápida, es como copiar un archivo sin restricciones. Una vez allí, los clientes tienen fácil acceso a una ubicación centralizada.

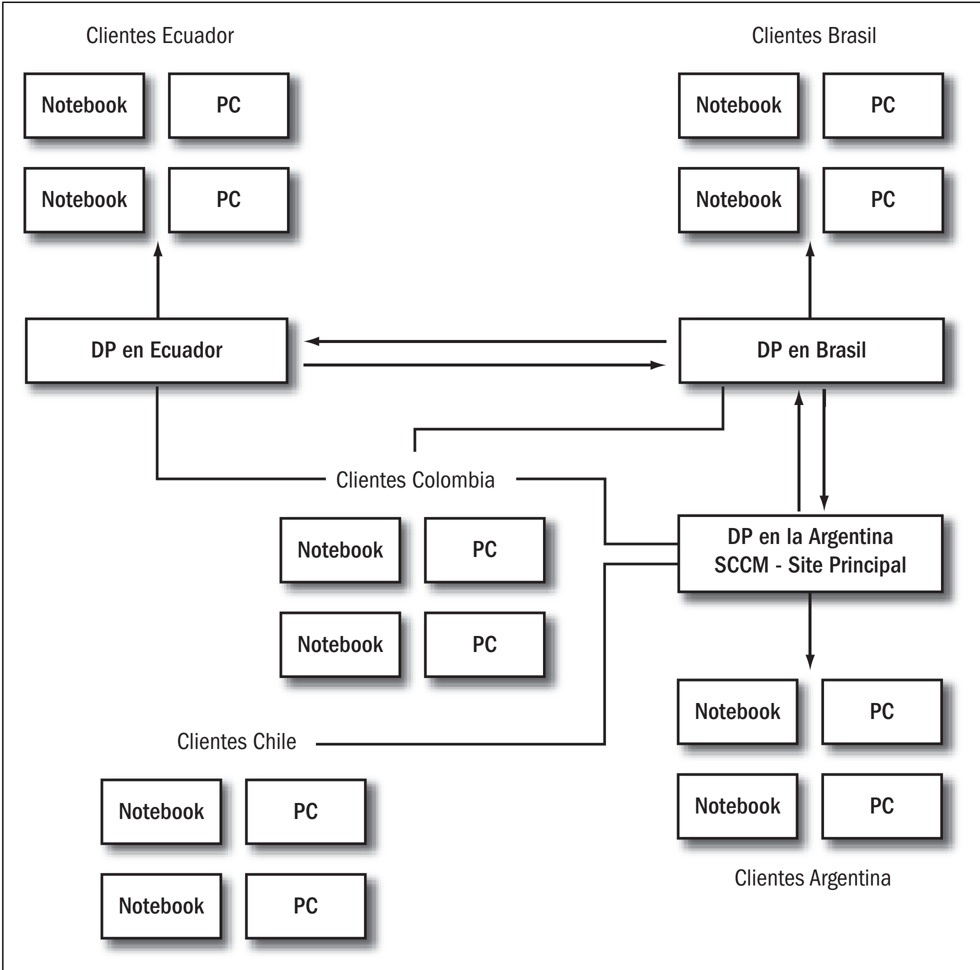


***Figura 6.** La figura muestra cómo debemos conectar nuestros clientes y los DPs según las conexiones que tiene la empresa en nuestro ejemplo.*

Para realizar un correcto análisis, es necesario conocer la red, para lo cual tenemos que monitorear los routers cada vez que distribuimos un paquete. Podemos empezar pruebas distribuyendo paquetes pequeños, e ir aumentando su tamaño para ver la reacción de la red. En donde el sistema se sature, instalamos un punto de distribución y volvemos a empezar las pruebas para determinar si la situación mejora. En conclusión, si vemos situaciones raras en la red que no podemos explicar, como desconexiones que se producen a menudo cuando se comienza a distribuir un paquete, conviene apagar el servidor principal de SCCM como primera medida y analizar lo sucedido.

Qué es un punto de distribución branch

Existen dos tipos principales de puntos de distribución: **estándar** y **branch**, con varias diferencias entre ellos que iremos analizando. Los puntos de distribución branch, en un principio, pueden instalarse en sistemas operativos de escritorio. Esto quiere decir que, teniendo Windows XP o 7, podríamos tener un punto de distribución económico y fácil de administrar. Los puntos de distribución branch trabajan con los puntos estándar. El equipo que oficia como branch baja el software pedido o los parches utilizando bits desde los DP estándar. Requiere de un punto de distribución estándar para poder funcionar. La distribución se realiza a demanda; esto quiere decir que, cuando un cliente del punto branch quiere un paquete, recién entonces el branch lo pide al punto de distribución estándar para bajárselo. Este tipo soporta cualquier clase de paquete, ya sea software, actualizaciones o sistemas operativos.

Estos puntos de distribución tienen algunas desventajas, entre ellas, no tienen un rol de SUP, lo que significa que no pueden escanear los clientes en búsqueda de actualizaciones. Pero la más importante es la restricción de conexiones: sólo soportan hasta 10 conexiones al mismo tiempo; o sea que sólo 10 clientes podrán bajar una actualización en un determinado momento. Si el cliente quiere conectarse y ve que todas las conexiones están ocupadas, vuelve a tratar de conectarse al mismo punto de distribución branch a los 30 segundos. Si no lo puede concretar, sigue buscando un nuevo punto de distribución.

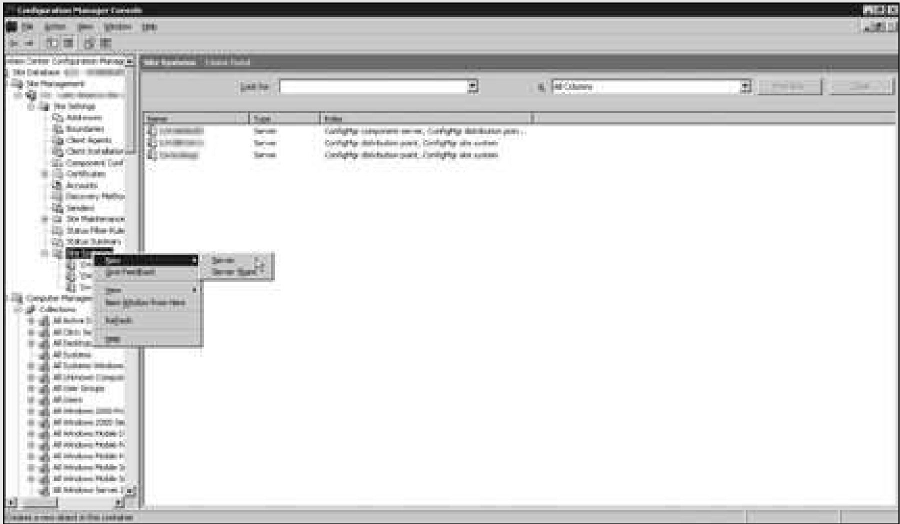
Cómo instalar un punto de distribución

La instalación de un punto de distribución es muy simple y la veremos en un **Paso a paso**. Como dijimos anteriormente, es muy importante hacer un análisis previo acerca de dónde instalarlo. También debemos tener en cuenta el espacio en disco necesario, porque los instaladores y parches irán a parar a un almacenamiento local en el nuevo punto de distribución. Es preciso hacer un análisis de expectativas de crecimiento antes de instalar el servidor. Luego, debemos ir a la consola de SCCM

y, en **Site Management/Nombre del Site/Site Settings/Site Systems**, ver todos los servidores de nuestra infraestructura. Haciendo clic derecho en **Site Systems**, podremos agregar un nuevo rol, como vimos anteriormente. La asignación del rol al servidor no hará más que crear una nueva carpeta compartida a la cual podrán acceder todos los clientes. El sistema de SCCM siempre la crea en el disco con mayor capacidad. En caso de que nos quedemos sin espacio, sólo necesitamos instalar un nuevo disco y listo; SCCM creará una nueva carpeta y empezará a copiar los archivos allí. Si queremos hacer espacio, debemos borrar la carpeta antes creada e instalar el nuevo disco. Esto regenerará la carpeta en la nueva ubicación sin tener pérdida de datos al poco tiempo.

■ Instalar un punto de distribución — PASO A PASO

1 Vaya hasta la consola de SCCM y elija el servidor en donde instalar el punto de distribución; posteriormente, si el servidor es nuevo, haga clic derecho en **Site Systems** y escoja la opción denominada **New/Server**.



►

HTA (HTML APLICACIONES)

Podemos crear aplicaciones mediante código HTML que ejecutará el IE con un programa llamado mshta. Es posible crear cualquier código HTML. Para convertirlo, hay que guardarlo con extensión HTA en vez de HTML; o en el tag **<HEAD>**, en el código, colocar **<HTA:Application ....>**. Se puede utilizar cualquier tecnología ya conocida: HTML/XHTML, VbScript, JavaScript, CSS, etc.

▶

2 Escriba el nombre del servidor nuevo, ingrese el nombre completo del equipo y el dominio en **Intranet FQDN**, elija la cuenta con la que va a instalar el rol y seleccione **Allow only site server initiated data transfer from this site system**, para que sólo el site sea capaz de iniciar una transmisión de información.



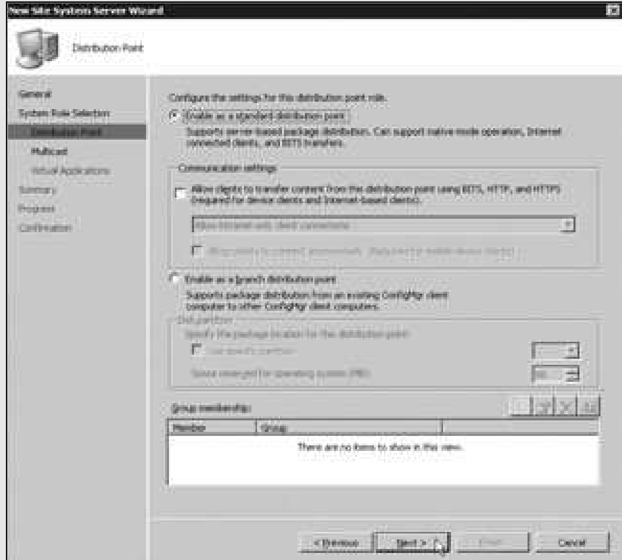
3 Presione en **Next** y verá los roles disponibles para instalar. Seleccione **Distribution Point**, márquelo y oprima el botón **Next.**



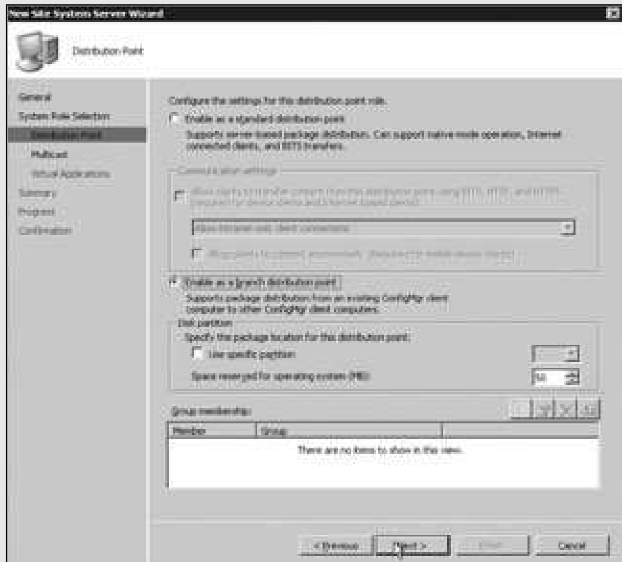
▶

▶

4 Seleccione la primera opción, llamada **Enable as a standard distribution point**, para instalar un punto de distribución estándar. Para continuar, deberá hacer clic sobre el botón denominado **Next**.



5 En caso de que desee instalar un punto de distribución branch, haga clic en **Previous** y posteriormente marque la opción denominada **Enable as a branch distribution point**. Oprima **Next** otra vez.



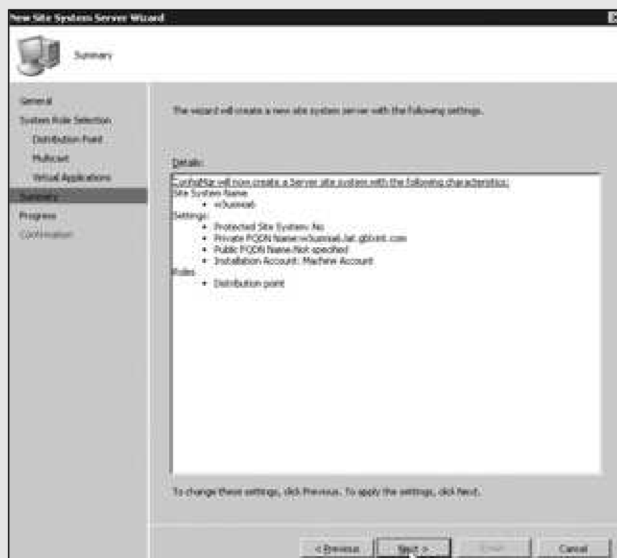
▶

▶

6 Marque la opción **Enable Multicast** si necesita trabajar con SCCM mediante Multicast. Luego, oprima **Next** y marque o no la opción **Enable virtual application streaming** para dar esta capacidad a las aplicaciones.

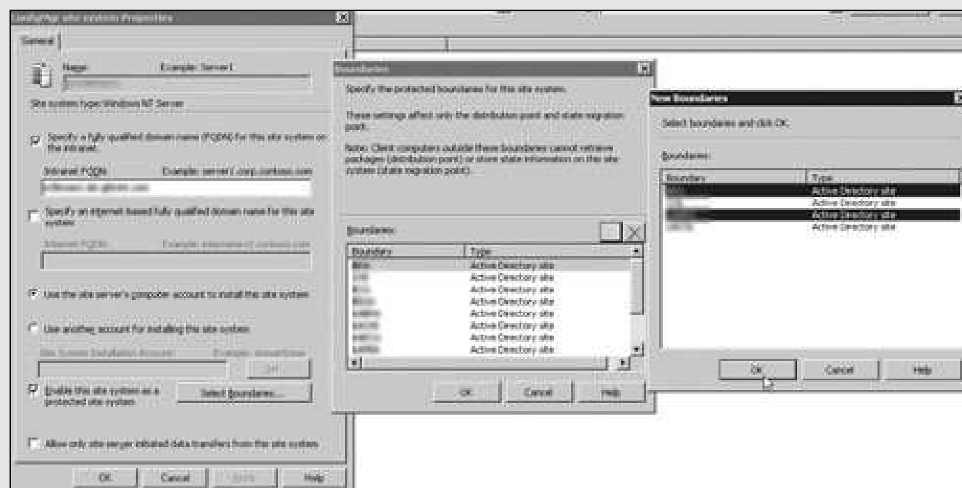


7 En este paso será necesario que haga clic sobre el botón llamado **Next**; de inmediato podrá ver el resumen y, cuando se completen las tareas, oprima el botón **Finish** para terminar el proceso.



▶

▶ 8 Puede segurizar el manejo de clientes luego si oprime **Site System**, que será un rol del nuevo servidor. Marque **Enable this site System as a protected site System** y haga clic en **Select Boundaries**. Allí elija el Active Directory Site que desea que el punto de distribución maneje.



Luego de instalar los puntos de distribución, éstos se pueden **proteger**. Podemos agrupar distintos grupos de clientes e indicarles que sólo pueden conectarse a algunos de los puntos de distribución que tenemos. En el ejemplo en el que teníamos que instalar un punto de distribución en Ecuador, lo más conveniente era decirles a los clientes de ese país que únicamente podrían conectarse al punto de distribución que figuraba allí o, en todo caso, a alguno más que tuviéramos en Colombia. Pero si no protegemos los puntos de distribución, podrían querer conectarse nuevamente a Argentina y otra vez tendríamos problemas. Esta configuración se realiza en las propiedades del DP y no en cada cliente. Entonces, vamos hasta el rol del servidor en Site Systems y lo configuramos indicándole las zonas de la red que se pueden conectar a él. De lo contrario podrán conectarse todos los clientes.



BOUNDARIES

Son zonas de DNS definidas en Active Directory para la red. En general, habrá una zona por país. Puede haber más, pero todas ellas pueden configurarse en SCCM para manejarlas. Dentro de **Site Setting/Boundaries**, es posible agregarlas. Las máquinas que no pertenezcan a los boundaries declarados no podrán administrarse por SCCM.

Posibles mejoras utilizando P2P

Hay algunas mejoras que pueden plantearse a partir de un pensamiento **P2P**. ¿Qué pasaría si cada máquina fuese un punto de distribución branch? Cada máquina podría ir pidiendo paquetes de actualizaciones a la de al lado. La hipótesis fue planteada en la universidad **In Holland**, de Holanda, donde querían saber cuál era la mejor forma y la más rápida de migrar toda su infraestructura de escritorio con Windows XP a Vista. SCCM tiene la capacidad de distribuir sistemas operativos, pero a su tiempo: alrededor de dos horas por equipo. La cantidad de máquinas está limitada porque consume gran cantidad del recurso de red. Esta universidad debía distribuir no sólo el sistema operativo, sino también los parches; estamos hablando de más o menos unos 25,6 TB de parches. La institución trabajó en conjunto con la compañía **Bittorrent Inc.** e implementaron una forma de distribuir parches utilizando una red P2P.

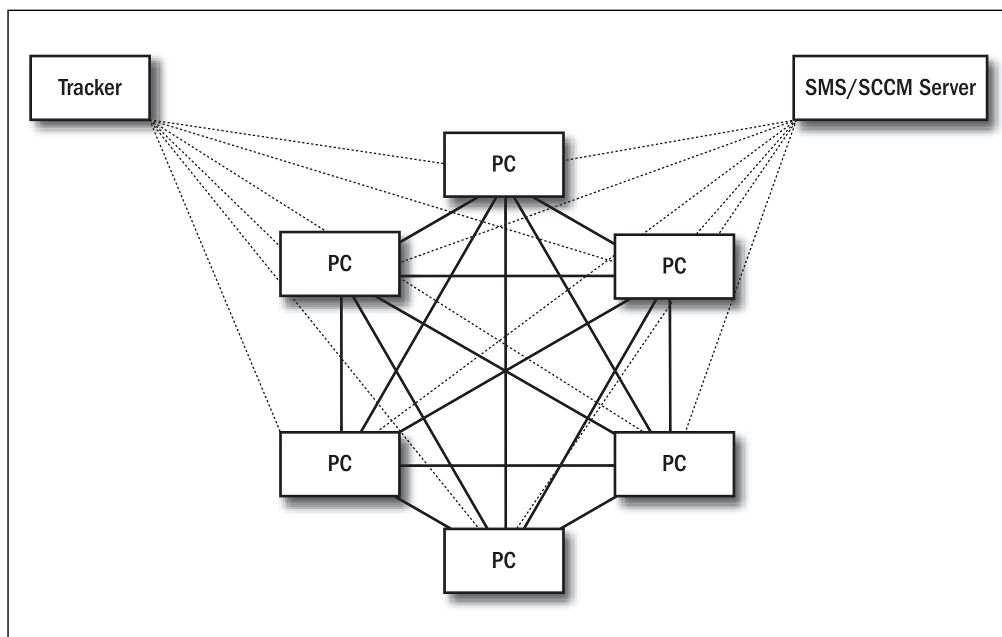


***Figura 7.** Los especialistas pudieron instalar un cliente P2P en cada máquina. Cuando una comenzaba a bajar archivos del sistema operativo a instalar, automáticamente empezaba a compartirlos con sus vecinas.*

Los participantes del experimento universitario obtuvieron resultados fantásticos. Repartieron los 25,6 TB de información a 6500 máquinas en 16 ubicaciones distintas en Holanda en tan sólo cuatro horas. Con la arquitectura de SCCM, hubiesen necesitado 20 servidores y cuatro días, mientras que con esta nueva implementación de SMS vía P2P utilizaron tan sólo dos servidores y el poder de los clientes. La solución fue implementada con un framework para .NET con licencia compartida del proyecto **GNU** y del **MIT**, utilizando el proyecto **Mono**. El resultado fue **Mono**

Torrent, anteriormente conocido como **BitSharp**. El framework brinda la posibilidad de crear todo tipo de recursos para manejar los torrents. La página del proyecto está en la dirección **www.monotorrent.com**. Este proyecto ya tiene dos o tres años, y en la actualidad encontramos soluciones parecidas, pero con licencia paga. Un ejemplo de esto es **Distribrute**, creada por la empresa **4M88**, que se fundó en el año 2008. Funciona con el mismo principio, pero está más enfocada en la distribución de sistemas operativos de forma rápida y sencilla utilizando el protocolo P2P. Su licencia cuesta sólo 5 euros por año y nos permite bajar actualizaciones. Ofrece soporte full y online, con accesibilidad vía e-mail, teléfono o escritorio remoto. **Leo Blom**, uno de los fundadores de 4M88, confirma que el grupo desarrollador está integrado por las mismas personas que trabajaron en In Holland como contratistas y que, luego, fundaron la empresa y comenzaron a trabajar en esta aplicación de gran éxito, vendiendo la aplicación cerrada. Son cuatro amigos los que integran el equipo, de ahí su nombre: abreviaron cuatro amigos (4 mates) en 4M88.

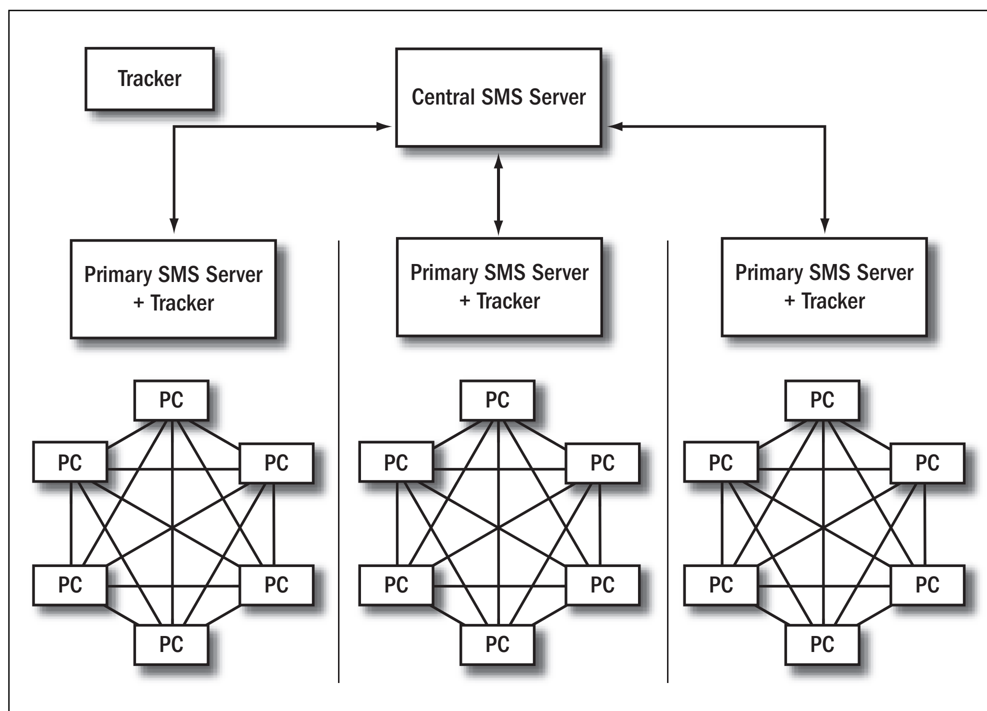


***Figura 8.** 4M88 logró integrar el poder de SCCM con una arquitectura P2P. Sin dudas, la fusión de SCCM con Bittorrent no tiene comparación.*

Según Leo, In Holland sigue usando la solución realizada mediante scripts y Mono Torrent. Distribrute puede instalarse con SCCM o por separado. Presenta algunas mejoras con respecto a la distribución de sistemas operativos con SCCM, que podemos ver en la siguiente tabla.

CARACTERÍSTICAS	DISTRIBRUTE	SCCM2007
Costos iniciales de la compra	Bajo	Alto
Contiene una gran cantidad de funcionalidades superfluas	No	Sí
Ocupa muy poco espacio en la infraestructura de TI	Sí	No
Pequeña incidencia cliente, más automatización	Sí	No
Es útil en entornos pequeños (menos de 500 computadoras de escritorio)	Sí	No
Permite ejecutar una reinstalación de escritorio masiva sin causar tráfico de la red	Sí	No
Instalación de la aplicación inmediata	Sí	No
Súper velocidad en despliegue de sistemas operativos y aplicaciones	Sí	No
Previsible llegada de los datos y el tiempo de instalación de la aplicación	Sí	No
No hay necesidad de servidores de sucursal	No	Sí
Facilidad de operación	Fácil	No fácil
Necesidades altamente cualificadas / administradores capacitados	No	Sí
Reduce el costo total de propiedad del servidor	Sí	No
Instalación inicial fácil	Sí	No
Fácil de corregir problemas	Sí	No
Todas las computadoras de escritorio son implementaciones de servicios de datos	Sí	No
Sistema operativo y aplicaciones se mantienen durante reinstalaciones	Sí	No
Reinstalación de escritorio es un proceso local	Sí	No
Reinstalaciones veloces	Sí	No
Reinstalaciones más confiables	Sí	No
Se puede realizar un ensayo previo en las horas de producción	Sí	No
Implementación de la eficiencia del protocolo	P2P	Multicast
Adaptaciones de infraestructura de red necesarias para utilizar el protocolo	No	Sí
Vulnerables a las interrupciones de red	No	Sí
Protocolo depende de la velocidad de los componentes de la red	No	Sí
La escalabilidad depende del número de equipos de sobremesa	No	Sí
Optimiza la implementación	Sí	NA

Tabla 4. *Diferencias entre Distribrute y SCCM 2007.*

Distribrute es la mejor opción para distribuir sistemas operativos, pues disminuye los costos y consumos. Para más información, podemos visitar **www.4m88.nl**.

P2P (PEER TO PEER)

Es un protocolo de red para compartir, usado por sistemas como Emule, Bittorrent y otros. Estos sistemas son conocidos por utilizarse en Internet, pero pueden aplicarse a la red privada. No bien comienza a consumir archivos, el cliente empieza a compartirlos, y no sólo puede bajar de un punto, sino que puede conectarse a varios clientes a la vez.

SYSTEM CENTER CONFIGURATION MANAGER 2007 R3

Debemos tener en cuenta que la versión R3 acaba de salir al mercado hacia fines de 2010. De esta forma, el caballito de batalla de Microsoft nos permite pensar en verde, ya que la principal característica de este producto es hacer un análisis de consumo de energía exhaustivo para todas las máquinas de una empresa, y brindar un resumen completo del consumo de las máquinas de escritorio, de los servidores y también de otros equipos asociados. Por otra parte, se encarga de incluir las licencias para realizar el manejo de los dispositivos móviles y también incrementa la cantidad de clientes que es capaz de manejar.

Características nuevas en R3

Hay algunas características nuevas que vale la pena explorar. Ahora podremos manejar hasta 300.000 clientes por site, y hay cambios en los métodos de descubrimiento y en todas las tareas en general. Sin dudas, la capacidad de **medir el consumo de energía de la empresa** es un gran logro de la gente de Microsoft. Con esta opción, podremos manejar políticas de energía para reducir consumos y bajar costos. Es necesario recordar que podremos monitorear el uso de una máquina y aplicarle una política que la coloque en estado inactivo hasta que vuelva a tener actividad. La versión R3 nos brinda una gran gama de reportes del consumo de energía de la empresa. Es capaz de trabajar con las nuevas capacidades de energía de los sistemas Windows 7, así como también con las de versiones anteriores del sistema. Para utilizar el control de energía, es necesario cumplir una serie de requisitos. En principio, el site principal debe tener instalado R3 y los equipos deben tener el cliente de SCCM R3 (la versión nueva), con lo cual, si decidimos instalar la nueva revisión, es preciso pensar en actualizar todos los clientes. Debemos tener en cuenta que el componente de **Hardware Inventory Client Agent** tiene que estar habilitado, pues se nutre de esa información. También los equipos deben tener instalado el agente llamado **Power Management Client Agent**.



CITRIX

Es la empresa pionera en virtualización de aplicaciones. Coloca todas las aplicaciones corporativas en el datacenter y las comparte a través de un servicio web. Mediante un navegador, podremos acceder a un archivo de Excel, a un cliente SAP o a una consola de SQL Server. Actualmente, tiene acuerdos entre Microsoft y Google para expandir sus soluciones.

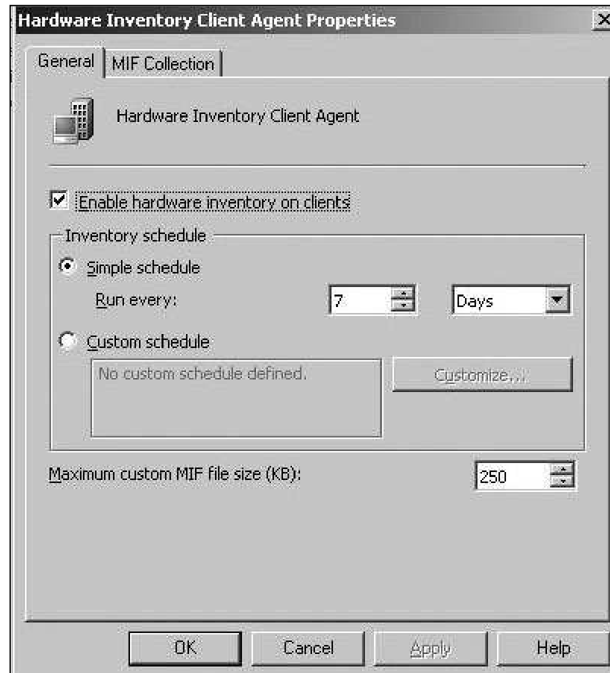


***Figura 9.** Podemos observar los agentes instalados en los clientes en **Site Settings/Client Agents**. Allí tendremos varios agentes, que son programas que se ejecutan en los clientes.*

Por último, el rol y la capacidad de Reporting Services deben estar instalados en el site. Por defecto, el agente de Power Management viene deshabilitado en SCCM R3, y debemos habilitarlo manualmente para utilizar esta nueva capacidad. Con la licencia de R3, se incluye la capacidad de manejar **System Center Mobile Device Manager**, que provee un control eficiente de dispositivos móviles Windows. Podremos administrar el uso de los teléfonos Windows, así como también distribuir aplicaciones mediante conexiones wireless. Es posible hacer todo lo que hacemos hoy con las máquinas de escritorio y servidores, manejar inventario, forzar políticas, y desplegar parches y software. R3 proporciona mejoras en el descubrimiento de Active Directory con una nueva característica llamada **Delta de Active Directory**. Ésta, combinada

{ } USUARIO SCCM LOCAL

En el grupo Administradores de los equipos será necesario que configuremos un usuario de dominio para SCCM. En este sentido es preciso tener mucho cuidado en conservar el password y no revelarlo, ya que podría cambiar cualquier configuración de los equipos de la red. Hay que agregarlo por GPO a todas las máquinas de la red.

con la capacidad **dynamic collection addition** (adicionar dinámicamente una colección), permite a los administradores reducir significativamente el tiempo en que se reflejan los cambios realizados en Active Directory y en las colecciones. Esto no reemplaza los tradicionales métodos de descubrimiento, sino que ayuda a que aparezcan antes los cambios recientes. Para finalizar, también trae una capacidad llamada **Prestaged Media**, una nueva manera de combinar una imagen de un sistema operativo booteable con una imagen instalable. Las tareas por ejecutar (**task sequences**) van grabadas en la imagen; entonces, por más que el equipo no disponga de red, podrá seguir utilizando esta característica.
SCCM 2012, también conocido como **Configuration Manager v.Next**, viene repleto de nuevas características. Está más centrado en el usuario y en brindarle herramientas centralizadas. Pretende unificar y simplificar la administración de los dispositivos utilizados por los mismos usuarios en la red, brindando aplicaciones inteligentemente y haciendo hincapié en el uso de aplicaciones virtuales. El acuerdo entre **Microsoft** y **Citrix** en 2010 tiene mucho que ver con este avance. También se unifica el uso de **User State Migration Tool (USMT)**, la herramienta para migrar perfiles de usuarios unificando más las herramientas dentro de System Center. La seguridad también juega un papel principal: la próxima versión de Forefront está basada en SCCM R2, con lo cual vemos la importancia que está cobrando esta herramienta en nuestra infraestructura y en la manera de solucionar los problemas cotidianos.

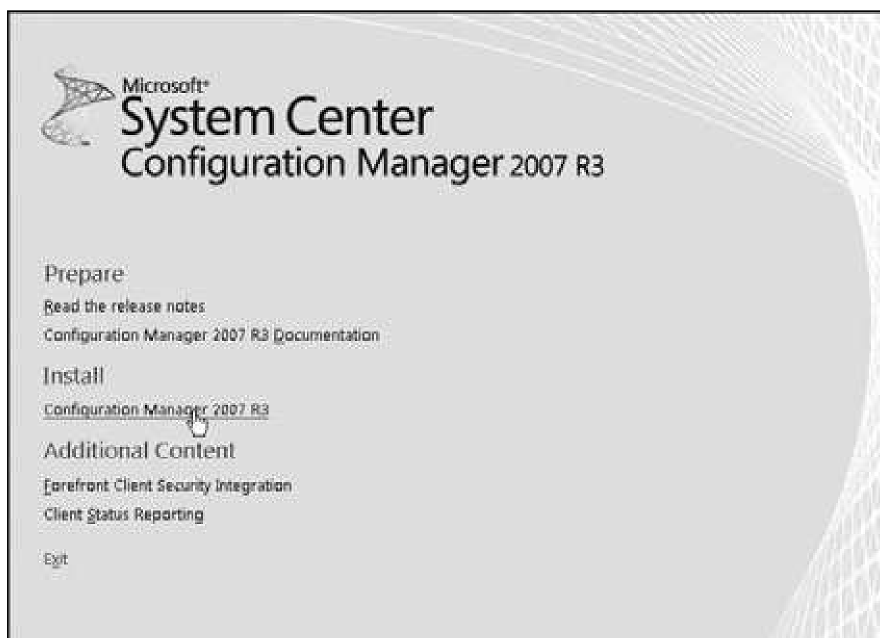


Figura 10. *La pantalla de bienvenida al comienzo de la instalación de SCCM R3 es muy parecida a la de versiones anteriores. Vemos la integración de Forefront para instalar.*

Sin dudas, la aparición del nuevo sistema operativo web **Google Chrome OS** –que funciona basado en la nube y con altas medidas de seguridad, sin necesidad de mantenimiento por parte de nuestra empresa, sino de Google–, plantea un nuevo desafío a Microsoft y a su visión de futuro. En su última presentación, **Google** hizo hincapié en que tiene un acuerdo con **Citrix** a partir del cual las herramientas corporativas podrán virtualizarse y quedar en el datacenter, con la seguridad que esto significa. De esta forma, podremos olvidarnos de los escritorios como hoy los conocemos. Esto también plantea un cambio drástico en la visión empresarial y en la de los activos de la compañía.



RESUMEN

Terminamos con la introducción al mundo de SCCM. Apreciamos que integra un conjunto de aplicaciones del cual es, prácticamente, la más importante. Vimos cómo instalar esta solución en nuestra empresa, los requisitos necesarios, la infraestructura que debemos adoptar y los roles. Luego seguimos con los clientes: aprendimos a instalarlos y analizamos los problemas que pueden presentarse. Pasamos a ver los detalles de los puntos de distribución, aprendimos por qué son tan importantes y cómo instalarlos. Repasamos algunos detalles de la nueva versión R3 y los focos de avance que se vienen. En el siguiente capítulo, continuaremos con SCCM.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 ¿Cuáles son los componentes de System Center?

2 Describa los prerrequisitos para instalar SCCM.

3 Mencione y describa los distintos roles que existen en SCCM.

4 ¿Para qué instalamos clientes en los equipos de la red?

5 ¿Cuáles son los prerrequisitos para instalar un cliente SCCM?

6 ¿De qué forma podemos comprobar y corregir errores en los clientes?

7 ¿Cuántos puntos de distribución necesitamos si tenemos una sucursal principal en Argentina y otra en Canadá?

8 ¿A dónde tenemos que ubicarnos para instalar un nuevo rol para nuestra infraestructura?

9 ¿Por qué se mejora la distribución en un sistema SCCM + P2P?

10 Enumere las mejoras que brinda SCCM R3.

EJERCICIOS PRÁCTICOS

1 Cree una red de prueba con un AD y elija un servidor de su red para instalar SCCM. Instale la base de datos y los roles, todo en un mismo equipo.

2 Configure el servidor SCCM y asigne a la red 10 máquinas de prueba.

3 Coordine la instalación de los clientes en los equipos y compruebe posibles fallas.

4 Instale la consola HTA para corregir los errores de los clientes. Adapte la herramienta a su red de prueba.

5 Asigne más clientes a su red habilitando los descubrimientos automáticos de SCCM.

Programas, parches e información

En este capítulo aprenderemos a utilizar las herramientas de SCCM y notaremos lo importante que son para nuestra organización. Veremos cómo crear colecciones de equipos, y repartir parches y programas a toda la empresa de una forma fácil y asertiva. También analizaremos lo mejor de SCCM, conoceremos los reportes, aprenderemos a utilizarlos, a modificarlos y crearlos.

COLECCIONES DE OBJETOS

Las colecciones de objetos nos permiten acotar el campo de acción de nuestras actividades, que se basarán en reportes, distribución de programas y parches. Los objetos que componen las colecciones son los clientes de SCCM instalados en distintos equipos seleccionados por alguna característica en común. De esta manera, también acotamos el campo de error de instalación, y los reportes son más concisos y exactos. Veremos que SCCM trae algunas colecciones preestablecidas de fábrica y, también, que podemos crear las nuestras con las características que se nos ocurran.

¿Qué es una colección?

Una colección de objetos en SCCM es una agrupación de equipos por alguna característica en particular o por un grupo de ellas. Tenemos varias colecciones predefinidas en nuestra consola principal de SCCM, pero podemos definir otras según criterios que se acomoden a nuestro negocio y requerimientos de casos particulares. Podemos acceder a las colecciones dirigiéndonos desde la consola principal a la ubicación: **SCCM/Site Database/Computer Management/Collections**.



***Figura 1.** La consola de SCCM es por demás amigable y fácil de utilizar. Del lado izquierdo tenemos las opciones, y del derecho, los detalles de cada una.*

Entre las colecciones predefinidas están: **All Systems**, **All Windows Mobile Devices**, **All Windows Servers**, **All Windows 2003 Servers Systems**, **All Windows XP Systems** y otras tantas más que veremos más adelante. Todas se centran en alguna característica en particular de los equipos; separan un grupo de ellos

del total de equipos en la compañía, de modo que tendremos distintos grupos según las tareas que debamos realizar. Por ejemplo, **All Systems** se centra sólo en dispositivos contactados por SCCM, tengan cliente o no, sean servidores, equipos de escritorio o teléfonos móviles; todos los dispositivos aparecerán en esa colección. **All Windows XP Systems** se basa en los mismos criterios, pero le suma la característica del sistema operativo Windows XP. O sea, debemos tener en cuenta que la colección se encargará de contener a todos los equipos de la empresa, tengan o no el cliente de SCCM, y que tengan el sistema Windows XP instalado.
Es interesante saber que algo similar ocurre con la opción llamada **All Windows Mobile Devices**, y así para las distintas colecciones existentes. Cada una de estas colecciones contendrá diversos equipos, para esto tendrá en cuenta cada uno de los criterios utilizados en su definición particular.
Más allá de las colecciones que trae SCCM por defecto, nosotros podremos crear las nuestras propias desde la consola. Las colecciones se construyen a partir de consultas a la base de datos. Es posible crear colecciones con un ayudante desde la consola principal, o importar una consulta ya creada y utilizarla para la definición. Lo recomendable es encontrar una colección que sea bastante parecida al resultado que buscamos, copiar la consulta SQL e ir modificándola hasta encontrar los resultados correctos. Es muy importante conocer las tablas y los campos de las tablas para efectuar las consultas, pero, como son demasiadas tablas, no es realmente necesario si nos basamos en las colecciones hechas y vamos comparando los campos. Veremos más detalles de las consultas SQL al finalizar este capítulo; a continuación, seguiremos analizando las particularidades de las colecciones.
Éstas son muy importantes para la administración de SCCM. Todas las acciones se realizan sobre la base de las colecciones de objetos y, también, sobre objetos individuales. Si quisiéramos repartir un software para las máquinas de escritorio pero no para los servidores, la única forma sería distinguir los destinatarios mediante colecciones. Los paquetes de parches y programas se informan a las colecciones. Si quisiéramos informar de un paquete nuevo de software a todos los dispositivos de escritorio, informaríamos sólo a la colección All Windows XP Systems o All Windows 7 Systems, que estamos seguros que son sistemas operativos de escritorio. La importancia de las colecciones también se da en los reportes que veremos



SISTEMAS OPERATIVOS WINDOWS

SCCM puede recopilar información, en equipos de escritorio, de Windows XP y 7, ambos en versiones Enterprise, Professional y Ultimate; de servidores Windows 2000 Professional y Server, Windows 2003 Enterprise y Standard de 32 y 64 bits, y Windows 2008 y 2008 R2, también Enterprise y Standard. Por supuesto, también de todas las versiones de Windows Mobile.

más adelante; es necesario acotarlos, por lo que también deben dirigirse a colecciones. Así, distinguimos los reportes de las workstations, de los correspondientes a servidores o cualquier otro tipo.

Es importante tener en cuenta que la principal función de las colecciones es encargarse de limitar y ordenar nuestro accionar; de esta forma pueden convertirse en un real apoyo para la tarea de administrar sistemas.

Más adelante veremos cómo las colecciones pueden crearse a gusto y solucionar problemas acotando el campo de acción. Por ejemplo, si tenemos una situación en la cual debemos saber qué máquinas de escritorio de la empresa tienen tan sólo 1 GB de memoria RAM, para expandir esa cantidad y así poder implementar un sistema administrativo sin dificultades, es interesante saber que podríamos sacar un informe de máquinas que tuvieran esas características realizando tan sólo una consulta u obteniendo un informe sobre la colección de workstations. Luego, para continuar, podríamos proceder a armar otra colección con estos resultados y, así, ir viendo características particulares de las máquinas de escritorio que sólo tienen 1 GB de memoria. Otro caso similar es si tenemos que repartir un software que demande muchos recursos de memoria, para lo cual deberíamos tener en cuenta estas máquinas, individualizarlas del resto y separarlas de la colección a la cual le distribuiremos el soft. Si quisiéramos actualizar los equipos, podríamos ir instalando las placas de memoria faltantes, teniendo en cuenta la necesidad de utilizar una colección para distinguirlas.

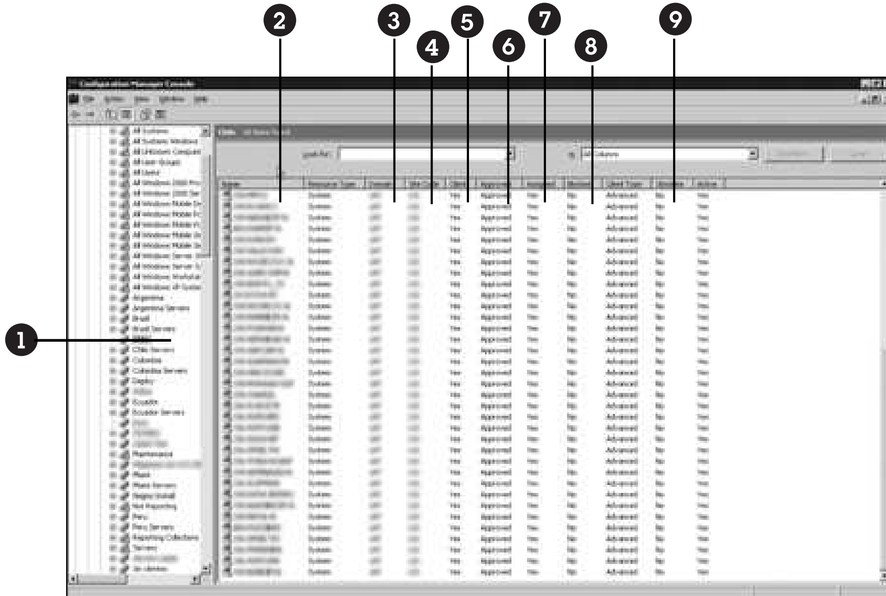
Veremos el avance de la tarea a medida que disminuyan los miembros de dicha colección. Éstos son algunos de los problemas que podríamos solucionar en nuestra empresa si tenemos SCCM configurado y funcionando. Sólo nuestra imaginación nos bloqueará situaciones que no se puedan resolver, pero casi siempre hay un camino para llegar a los resultados buscados. Debemos saber que ésta es una herramienta muy flexible, poderosa, fácil de utilizar y muy sencilla para aprender a manejar. Por estas razones resulta una gran ayuda para la administración que debemos hacer de los sistemas de la empresa y también es muy importante para generar información que pueden utilizar gerentes, arquitectos y analistas. Presentamos a continuación una guía visual de una colección en la cual nos encargamos de detallar algunos de los datos que podemos obtener a simple vista.



PRIMERA DIVISIÓN DE ADMINISTRACIÓN

La administración de servidores y de máquinas de escritorio nunca depende del mismo departamento. Tendremos un departamento de IT y uno de Helpdesk. Al primero le resultará interesante conocer información de los dispositivos servidores, pero no de las máquinas de escritorio, a diferencia de lo que ocurre con el Helpdesk. Las colecciones ayudan a separar y agrupar.

Datos de clientes en colecciones GUÍA VISUAL



❶ **Nombre de colección:** desde esta sección es posible que acceder a todas las colecciones que se encuentran disponibles en nuestro SCCM.

❷ **Nombres de equipos:** en esta columna se encuentran los nombres de los equipos que componen la colección correspondiente.

❸ **Dominio:** en esta columna se muestra el dominio de cada equipo.

❹ **Site:** se trata del código del site configurado en cada cliente. Recordemos que el nombre del site siempre es de tres letras.

❺ **Cliente:** en esta columna encontraremos información que nos indica si el cliente de SCCM está instalado o no en el dispositivo.

❻ **Approved:** puede ser que, por ciertas razones de seguridad, al instalarse el cliente no se aprueben determinados equipos para la recaudación de información, parches, etc.

❼ **Assigned:** esta columna se encarga de mostrarnos si el cliente tiene asignado un site o si no lo puede alcanzar en la red.

❽ **Blocked:** aquí figuran los equipos que deseamos bloquear.

❾ **Obsolete:** en esta columna encontraremos información sobre si el equipo está o no considerado como obsoleto. Esto quiere decir que SCCM no recibe información ni conexión con el cliente durante meses.

Las colecciones de SCCM pueden crearse a partir de una selección de objetos de Active Directory. Por ejemplo, tendremos una colección llamada All Users, que contendrá a todos los usuarios del AD. SCCM usa esta información para realizar

informes y cruces de datos; también completa los datos necesarios para efectuar reportes y análisis. Para crear una colección de este tipo, podemos generar una OU con los objetos que queremos administrar desde SCCM por alguna característica particular que podemos distinguir con una consulta de AD. Entonces, luego de crear la OU, creamos la colección basándonos en ella.

Colecciones nuevas y por defecto

Ahora exploraremos un poco las colecciones predefinidas que trae SCCM, y también aprenderemos a crear otras nuevas. Las colecciones por defecto se llaman **Builtin Collections** (colecciones incorporadas). Son un gran número de colecciones predefinidas por Microsoft en SCCM, que se generan con la instalación de la herramienta. Las veremos en la siguiente figura; son las que contienen un candado como decoración de los iconos.

***Figura 2.** En la imagen vemos las Builtin Collections con un candado. Las que no tienen candado están creadas posteriormente.*

BUILTIN COLLECTIONS EN SCCM R3

Debemos tener en cuenta que en la revisión número tres, Microsoft se encargó de agregar algunas colecciones preestablecidas nuevas que no estaban en R2. Por ejemplo, podemos nombrar la aparición de dos colecciones denominadas **All NO Power Policy** y **Apply Default Policy**, para el manejo de políticas de la energía de los equipos.

Hay bastantes colecciones preestablecidas, pero seguramente necesitaremos más para nuestra administración. Cada empresa es un mundo distinto, con ciertas características que la hacen individual en determinados rasgos. Con la instalación de SCCM, podemos distinguir todos los Windows Server 2000 o 2003, por ejemplo, o los dispositivos con Windows Mobile, pero podemos crear nuestras propias colecciones para lograr un mayor aprovechamiento del sistema según nuestras necesidades.

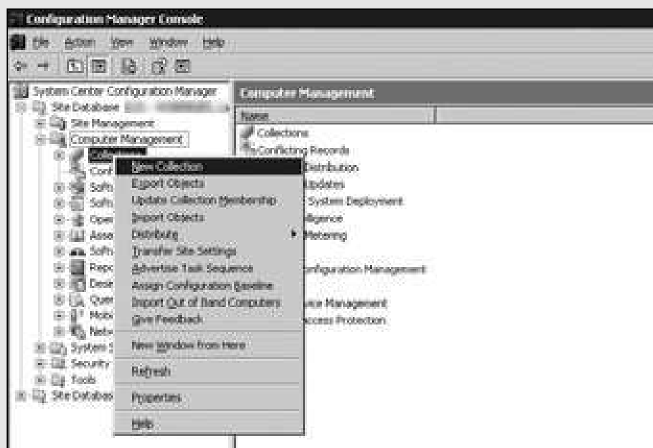
Para crear colecciones existen muchas formas, pero las más utilizadas son tres:

- A partir de una consulta al AD o de grupos de AD.
- Mediante una consulta a la base de datos de SCCM.
- Mediante una consulta por alguna característica (por ejemplo nombre, IP, etc.) desde los ayudantes de SCCM.

Tanto la primera como la última generan colecciones estáticas, en donde siempre aparecerán los mismos miembros. El ayudante de SCCM para generar colecciones nos da la posibilidad de hacer un filtro de todos los equipos registrados en la consola y elegir cuáles queremos que conformen la colección. En cambio, la segunda opción genera una colección dinámica, en donde cada determinado tiempo se hace una actualización, realizando la consulta que la define a la base de datos. Veremos esta distinción de colecciones más adelante. Ahora aprenderemos a crear una colección a partir de un grupo de AD.

■ Crear una colección a partir de una consulta de AD — PASO A PASO

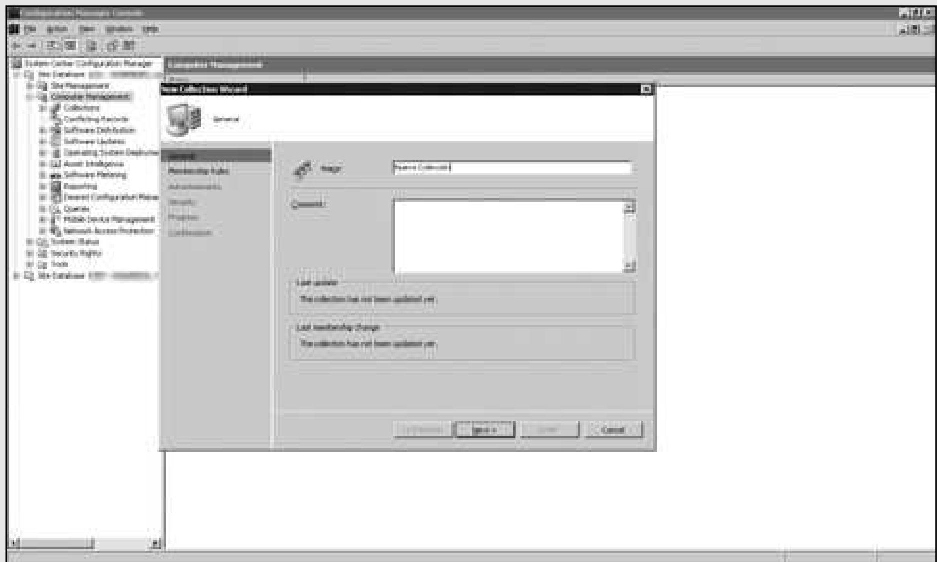
1 Diríjase a la consola de SCCM. Vaya hasta **Collections**, haga un clic derecho y seleccione **New Collection** para iniciar el asistente.



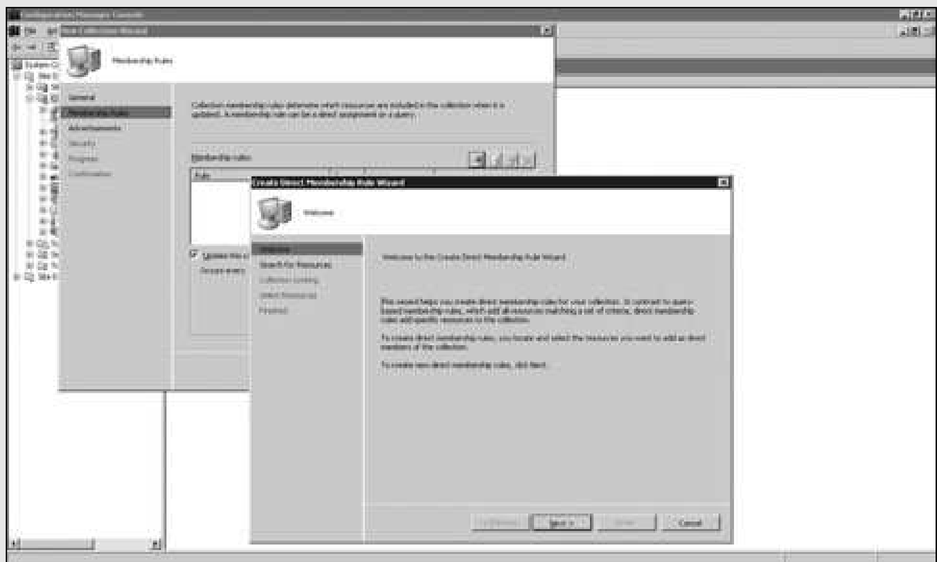
▶

▶

2 Para continuar, en la ventana emergente será necesario que coloque un nombre distintivo para la colección que está creando y también un comentario o descripción sobre ella; de esta forma podrá identificarla posteriormente.

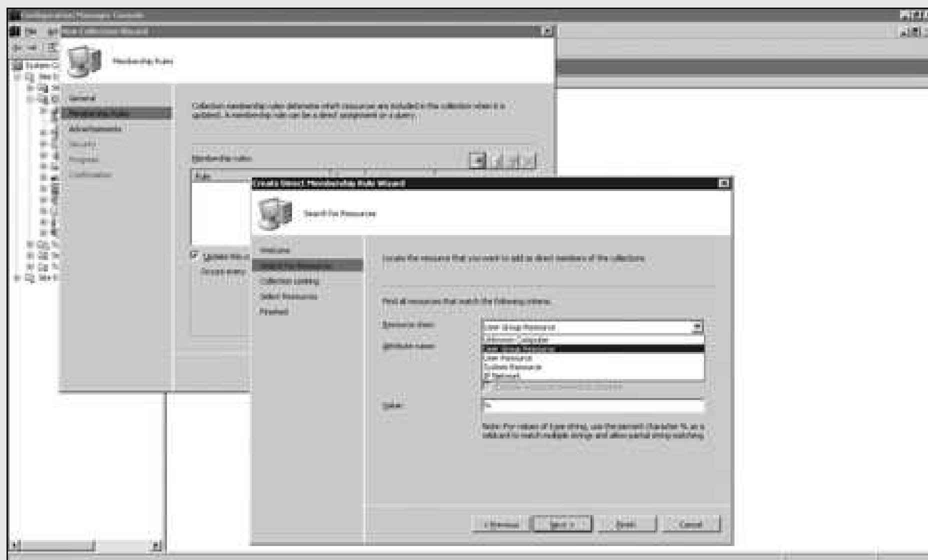


3 Elija las reglas que conformarán la colección; puede haber varias de distintos tipos. Haga clic sobre el icono de la computadora; se abrirá otra ventana emergente, vea la información y oprima **Next**.

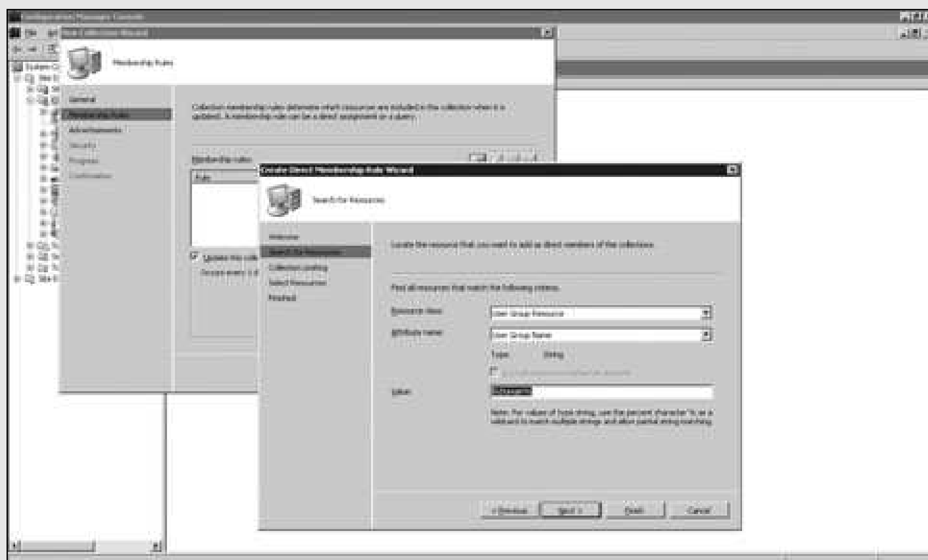


▶

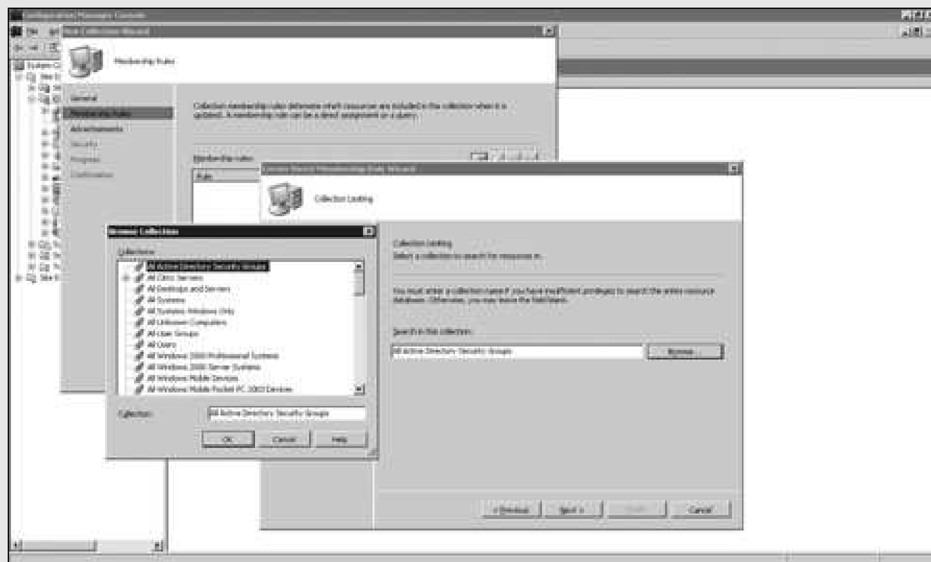
4 En este paso es necesario que elija una de las cinco clases de recursos presentadas en la ventana para seleccionar; para este ejemplo deberá optar por la clase denominada **User Group Resource**.



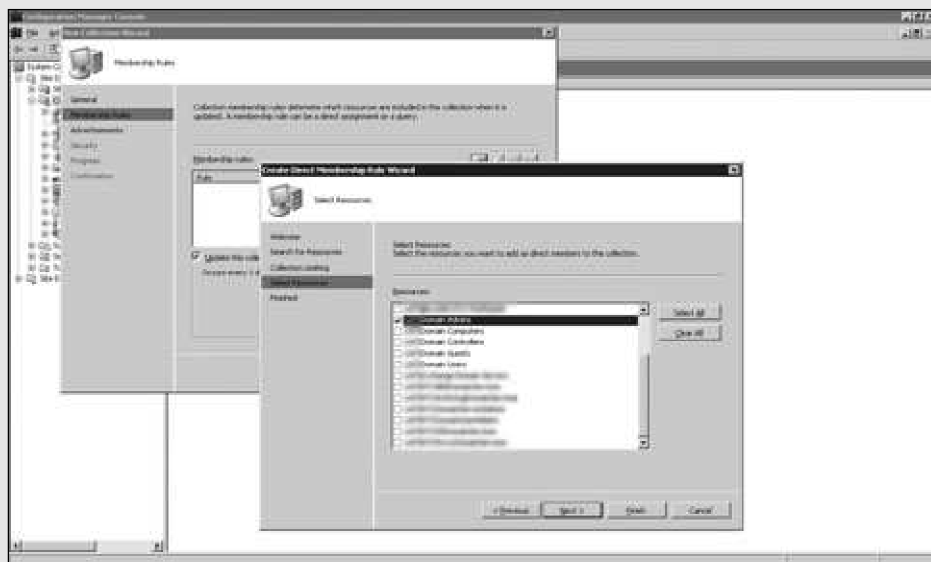
5 De la lista desplegable, escoja una de las 14 opciones disponibles. Para el ejemplo, seleccione **User Group Name**. En **Value** ingrese un nombre y, para buscar, escriba **%Domain%**.



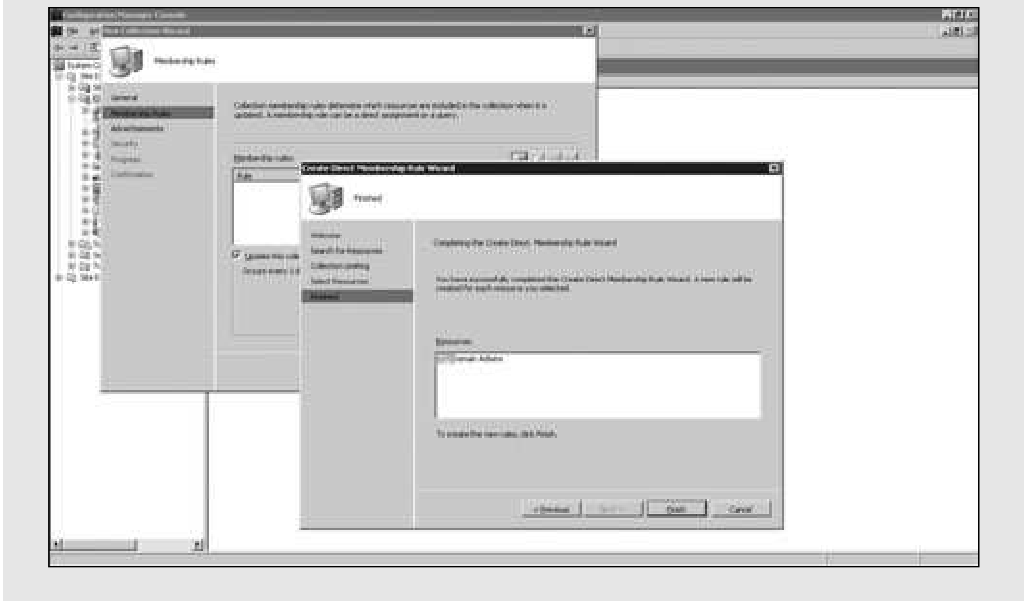
6 Haga clic sobre el botón llamado **Next** para continuar. Aquí deberá colocar una colección si quiere acotar la búsqueda. Oprima sobre la opción **Browse** para ver un listado de los posibles valores.



7 Podrá darse cuenta de que aparecerá un listado que contiene todos los valores que posean la palabra **Domain**; desde este listado deberá seleccionar el que esté buscando y posteriormente oprimir el botón **Next**.



▶ 8 Observe el resumen y pulse **Finish**. Luego, haga un refresco en **Collections** y verá la colección recién creada. Posiciónese sobre ella para ver los miembros.



Existen muchas opciones para crear el filtro antes mencionado, pero, seguramente, encontraremos una que nos sea útil. Podemos tener más de una regla para generar el filtrado; de esta forma, SCCM nos da mayor flexibilidad. Al seleccionar la colección, ésta estará conformada sólo por los miembros que hayamos filtrado.

Colecciones estáticas y dinámicas

Existen colecciones estáticas y dinámicas. Llamaremos estáticas a aquellas que no cambian con el correr del tiempo, en tanto que dinámicas son aquellas a las que se suman miembros o en las que se los descarta a cada momento automáticamente; por ejemplo, las definidas con una consulta a la base de datos antes mencionadas.



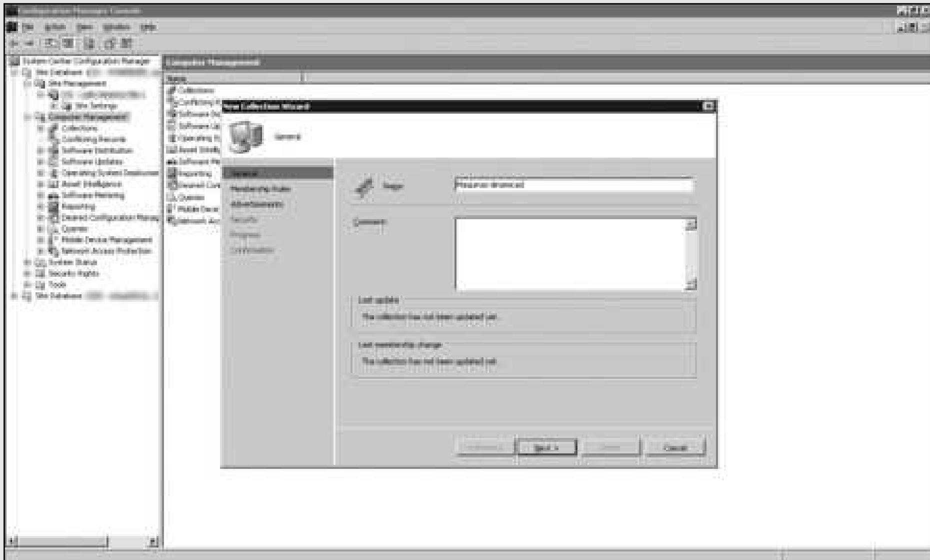
TRANSACT SQL

Debemos tener en cuenta que hay varios lenguajes de consultas para bases de datos, y uno de ellos es el llamdo Transact SQL. Éste es usado por Microsoft en sus motores de bases de datos y en sus lenguajes de programación para embeber código SQL. La empresa Sybase también es propietaria de esta extensión del lenguaje SQL.

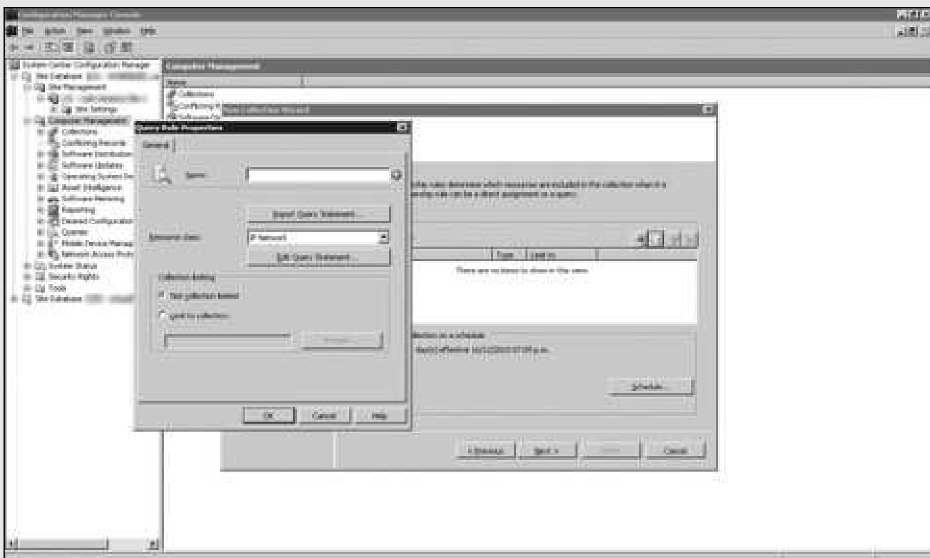
Vimos que una colección se puede formar eligiendo equipos por alguna característica en particular. Es posible crear colecciones eligiendo los nombres de los equipos, o las direcciones IP o MAC. Una colección estática es aquella en donde se elige una clase de recursos, se escoge un recurso de esa clase y se aplica un filtro para realizar una búsqueda en las colecciones que cumplan con todos estos requerimientos. Una vez que lo hacemos, vemos un listado y seleccionemos los datos correctos. Estas colecciones no cambian con el correr del tiempo y siempre están formadas por los mismos equipos.
Estas colecciones, estáticas y dinámicas, nos servirán para distintas situaciones. Es una gran ayuda que podamos crearlas para acaparar soluciones de todo tipo en nuestra tarea de administración. Vamos a ilustrar este tema con un ejemplo, para entender mejor la diferencia entre estas dos colecciones. Por ejemplo, imaginemos que queremos repartir parches a todos los servidores de la empresa. Para esto, hacemos una nueva colección que abarque todos los sistemas operativos Windows Servers y la llamamos Servidores Windows. Efectuamos una consulta; por lo tanto, es una colección dinámica. El resultado es que, siempre que instalemos un nuevo sistema operativo Windows Server y tome contacto con SCCM, el equipo pasará a integrar esta colección. Ahora, podemos preguntarnos qué ocurriría si quisiéramos una colección para realizar pruebas de parches antes de instalarlos masivamente en toda la empresa. En este caso, deberíamos definir un servidor representante de cada tecnología en la compañía y colocarlo en una colección. Cuando decimos "representante de cada tecnología", nos referimos, por ejemplo, a un servidor SQL, uno de antivirus, uno de algún sistema CRM, etc. Esta nueva colección, llamada por ejemplo Windows testing, será una subcolección de Windows Servers, pero será estática. ¿Por qué? Porque no podríamos cambiar todos los meses de servidores de pruebas, sino que deberíamos tenerlos bien controlados e individualizados. Podríamos elegir los equipos que conformarán la colección mediante nombre, IP o alguna otra característica. De esta manera, sólo ellos conformarían la colección Windows Testing. Así queda reflejada la diferencia y la importancia de cada tipo de colección.
La colección de testing nos permite hacer las pruebas de los parches para luego, lanzar la instalación al resto de los servidores, de modo que ninguno quede sin parches si definimos la colección de servidores como Windows Servers. A continuación, veremos cómo generar una colección dinámica mediante una consulta SQL. Debemos tener conocimientos de SQL avanzados para realizar este procedimiento.
Con este paso a paso, se generará una colección que cambiará cada determinado tiempo. Si nuestra consulta SQL trae los equipos que no tienen el cliente SCCM instalado, a medida que se vayan instalando, la colección se reducirá, y si hay algún fallo general, es posible que aumente el número de miembros. Su tamaño se vuelve flexible, a diferencia de lo que ocurre con una colección estática; es decir que puede crecer o disminuir en número de miembros.

■ Cómo crear una colección dinámica — PASO A PASO

1 En primer lugar diríjase a **Collections**, haga clic con el botón derecho del mouse y seleccione **New Collection**. Escriba el nombre de la nueva colección.



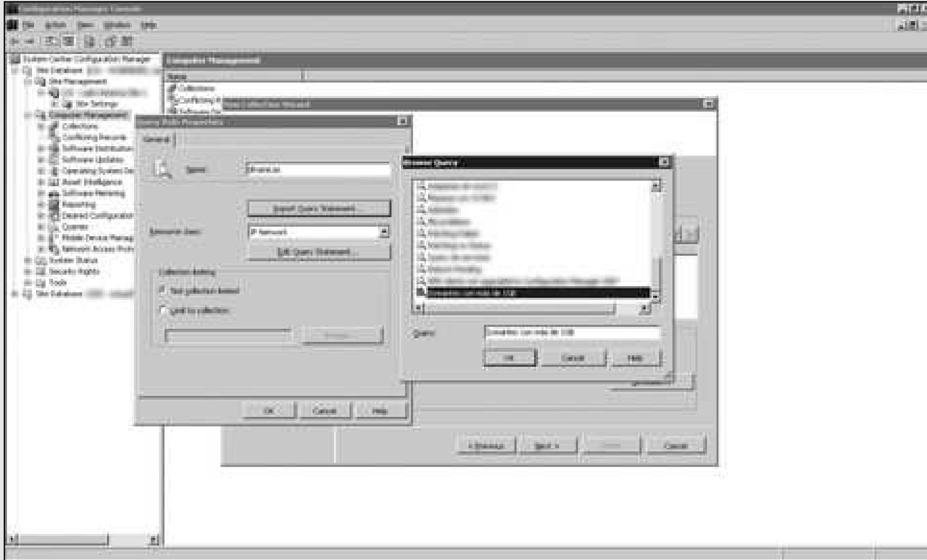
2 Oprima **Next** y elija las reglas que conformarán esa colección. En vez de la computadora, seleccione el cilindro amarillo. Se abrirá una ventana emergente para definir una consulta de SQL. Escriba una que traiga los equipos que usted desea.



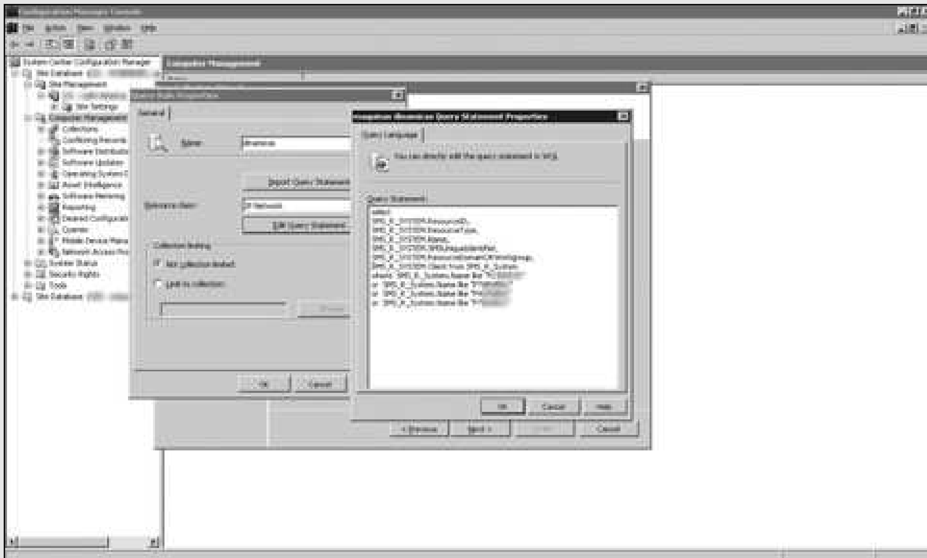
▶

▶

3 Para continuar escriba un nombre para la consulta. Puede crearla desde una importación o ingresando código Transact SQL. Oprima **Import Query Statement**. Elija una colección y presione el botón llamado **OK**.

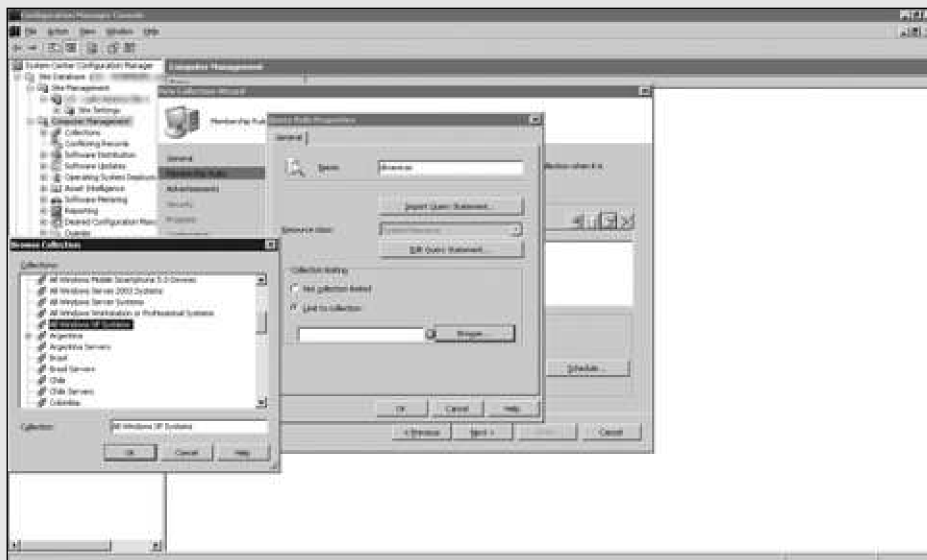


4 Si oprime sobre la opción llamada **Edit Query Statement**, verá el código SQL correspondiente; debe tener en cuenta que más adelante podrá obtener detalles sobre esta interesante característica.

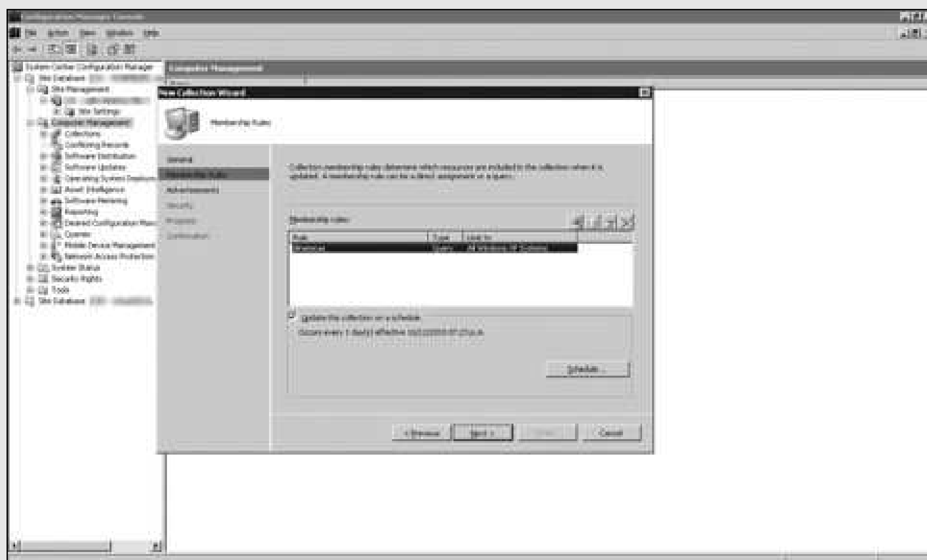


▶

5 En el recuadro denominado **Collection limiting** puede proceder a limitar la búsqueda de equipos a una colección específica. Para realizar esta tarea oprima el botón **Browse** y luego elija una colección del listado.

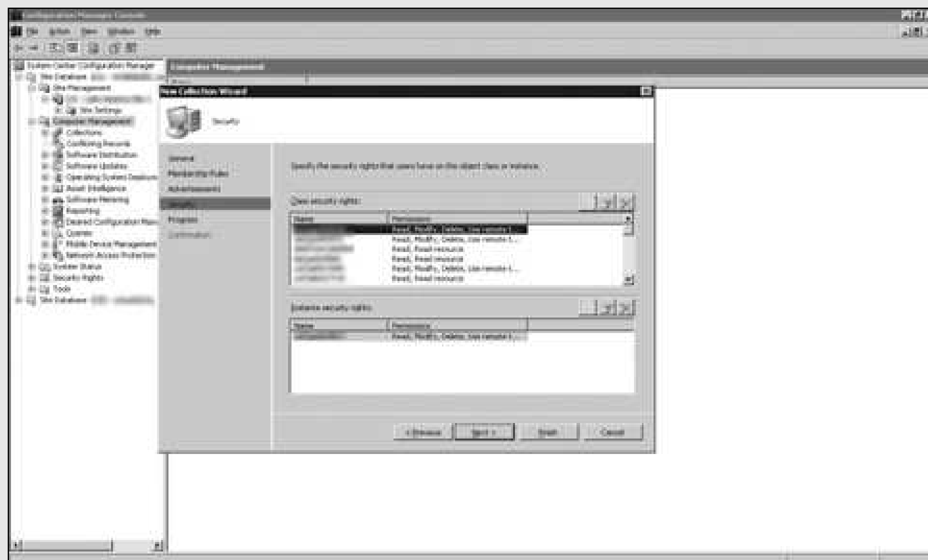


6 Para continuar, cree otra política si lo considera necesario o deje solamente la anterior. Seleccione **Update this collection on a Schedule** y configure la programación si lo desea. Luego, pulse sobre el botón llamado **Next**.

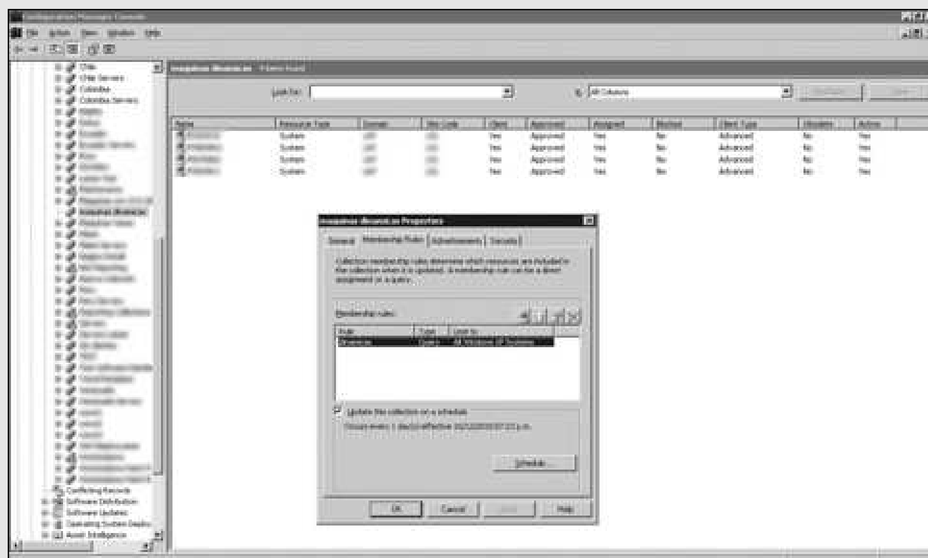


▶

7 Podrá ver un listado completo de advertencias, pero como la colección es nueva, este listado se encontrará vacío. Oprima el botón llamado **Next**. Vea el resumen de seguridad y presione **Finish** para crear la colección.



8 Para continuar deberá ir a la opción **Collections** y oprima **F5** para actualizar. Diríjase hasta la colección recién creada, haga clic derecho y seleccione **Properties** para ver y/o modificar los parámetros.



PAQUETES DE SOFTWARE

Estuvimos viendo cómo crear las colecciones de equipos para dividir la administración del sistema SCCM de nuestra empresa. Parte de la administración es repartirles programas. Ahora veremos cómo distribuir software a estas colecciones. Éste es el principal objetivo de SCCM, junto con la distribución de parches y los reportes. Si tenemos un programa empresarial con una nueva versión, SCCM nos será muy útil para que todos los dispositivos lo obtengan muy rápidamente. Sólo debemos crear un instalador, distribuirlo y analizar el progreso de su instalación.

Instalar un paquete de software en el servidor

Es muy importante entender lo que significa poder repartir un software en forma masiva a toda la empresa. Imaginemos compañías soportadas por tecnología antigua y que no puedan tener esta capacidad que brinda SCCM. Si necesitáramos repartir un cliente del famoso sistema empresarial SAP, por ejemplo, los recursos del departamento de Helpdesk tendrían que ir máquina por máquina instalando el cliente, interrumpiendo al usuario y ocupando durante unos minutos cada equipo. Es inmensa la cantidad de tiempo que se requiere para terminar la implementación de un nuevo software. Este tipo de prácticas cansa a los administradores, quienes entonces dan permisos de administración local a los usuarios para que instalen cualquier programa. Claro que esto origina una gran falla de seguridad, ya que podemos encontrarnos con software no probado ni avalado por ninguna norma de seguridad. Es más, los empleados pueden instalar virus sin darse cuenta, y provocar así una cadena de infección sin retorno en toda la red de la empresa, con enormes pérdidas monetarias. Con SCCM, simplificamos la distribución del software corporativo, al controlar no sólo la seguridad, sino también las licencias. En esta sección del libro aprenderemos a crear un paquete de instalación de software y a repartirlo para miles de clientes al mismo tiempo.

El primer paso en una distribución de software es preparar el paquete en el servidor. Debemos copiar los archivos de instalación en el servidor principal de SCCM, en una carpeta local. Luego, SCCM se encargará de colocarlo en una carpeta compartida a la que puedan acceder todos los clientes. Por lo general, los instaladores de software deben obtener las respuestas del usuario para la instalación. Mediante el uso de scripts, podemos obviar esta interacción con el usuario, para no obstruir el trabajo diario. También, si obstruir un poco el trabajo diario no afecta demasiado a la compañía, es posible mandar a instalar un software de manera tradicional, mostrando al usuario cada pantalla del proceso. Hay una opción en el armado del paquete que veremos más adelante, en donde elegiremos ocultar o no los mensajes.

Si utilizamos un script de instalación, podemos realizar todo tipo de acciones, y hay una larga lista de acciones que podemos llevar a cabo. Necesitamos tener

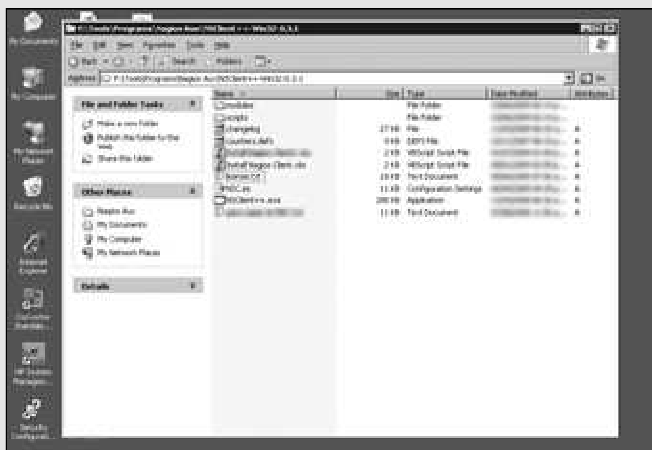
conocimientos de VBscript, un lenguaje de Microsoft para scripting. Entre las más utilizadas podemos nombrar:

- Verificación de versión antes de instalar, para saber si es correcta y proceder.
- Posibilidad de generar una carpeta en alguna otra ubicación que no sea la creada por default (primera regla de seguridad).
- Acceder a la verificación del espacio en disco para no obtener errores posteriores en medio del proceso de instalación de la aplicación.
- Actualizar un software pero ejecutando un desinstalador en caso de encontrar un antivirus viejo instalado y, luego, ejecutar el instalador del nuevo antivirus.

Al armar el paquete, se seleccionan programas para ejecutar. Podemos elegir el instalador por default de MSI o un script. También es posible ingresar más de un script para realizar una tarea tras otra. Ésta es una forma de reutilizar código ya programado para efectuar algún chequeo. También podemos crear distintos instaladores con el mismo paquete. Tenemos la posibilidad de tener instaladores diferentes si queremos instalar una versión completa o una más restringida, según haya una diferencia de usuarios. Al crear el paquete, SCCM genera una carpeta compartida en su sistema de carpetas. Cada punto de distribución tiene una carpeta principal compartida a nivel sistema (oculta), de donde cuelgan todas las demás carpetas de software y parches que vayamos generando. A continuación, veremos cómo construir un paquete de software para distribuir.

■ Crear un paquete de software para distribuir — PASO A PASO

1 Busque la carpeta de instalación de un software cualquiera. Cópiela localmente al servidor de SCCM con todos sus paquetes.



►

▶

2 Cree un script de instalación del software en cuestión. Coloque el script en la misma carpeta de instalación local anteriormente copiada.

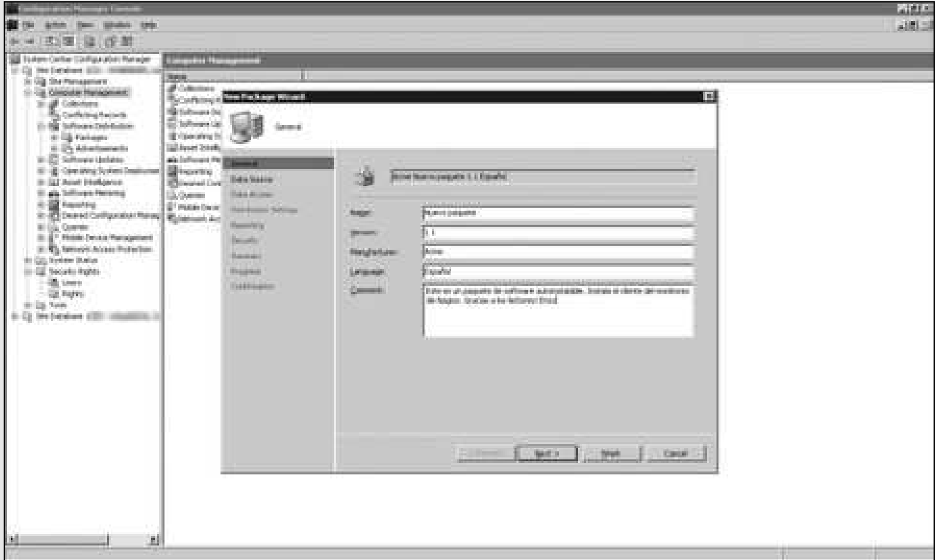
3 Vaya a la consola de SCCM. Diríjase a la opción denominada **Site Database/Computer Management/Software Distribution/Packages**. Haga clic con el botón derecho del mouse en esa carpeta y elija **New/Package**.

▶

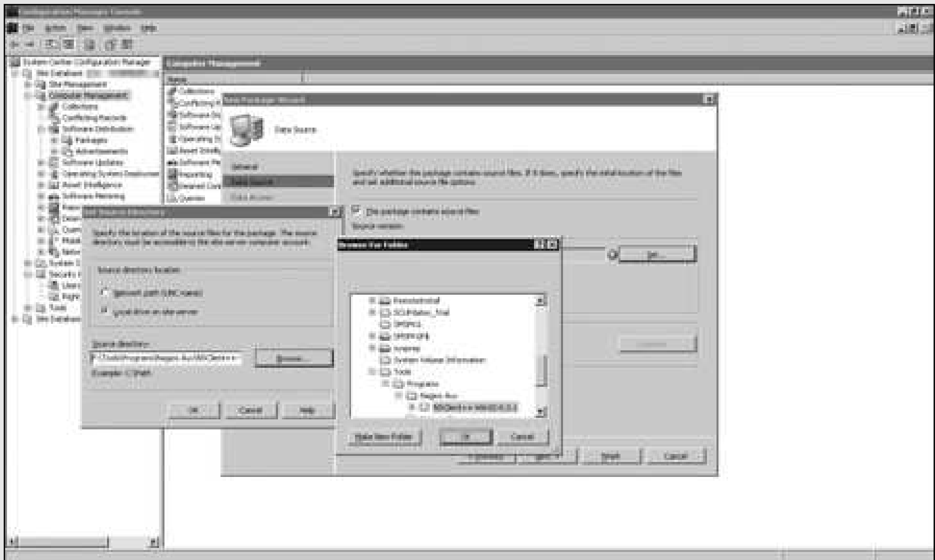
VBSCRIPT

Debemos tener en cuenta que VBScript es un lenguaje interpretado por sistemas operativos de la familia Windows, una variación de Visual Basic de Microsoft. Es una herramienta potente para la automatización de tareas de administración sobre estos sistemas. Es muy utilizado en programación ASP, y su principal competidor es el lenguaje JavaScript.

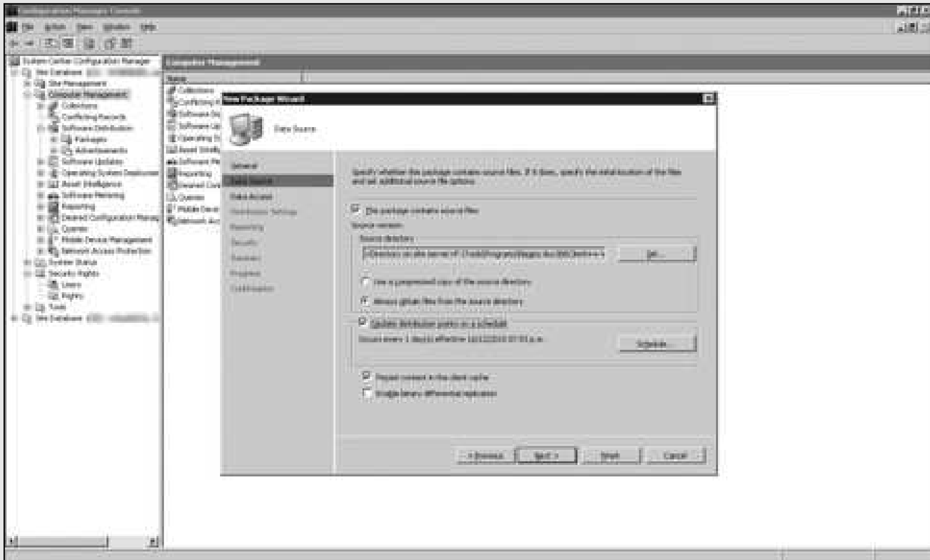
4 Para continuar, en la ventana emergente del ayudante, escriba un nombre, un detalle de la versión, el fabricante, el lenguaje y observaciones si las hubiese. Luego, oprima el botón denominado **Next**.



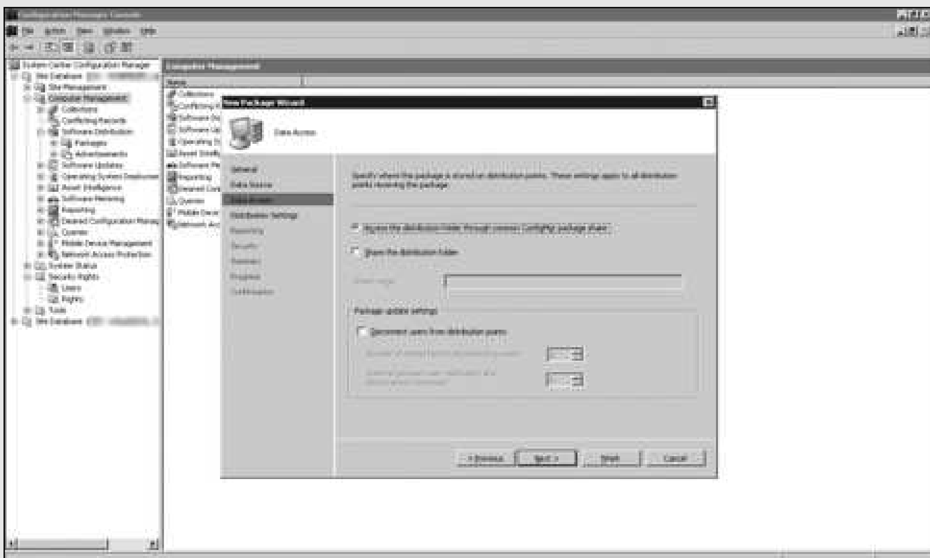
5 En esta ventana elija la fuente de los archivos del paquete. Oprima **Set**; en la ventana emergente seleccione **Local drive on site server** y presione **Browse** para ubicar la carpeta que contiene el instalador.



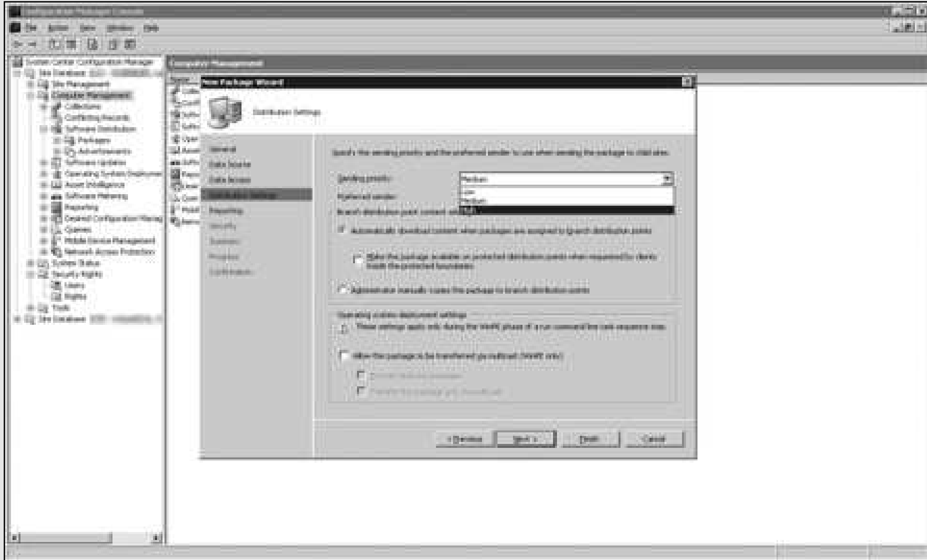
6 Asegúrese de que esté seleccionado **Always obtain files from the source directory**. Seleccione **Update distribution points on a Schedule** y también **Persist content in the client cache**, salvo que el paquete sea muy grande.



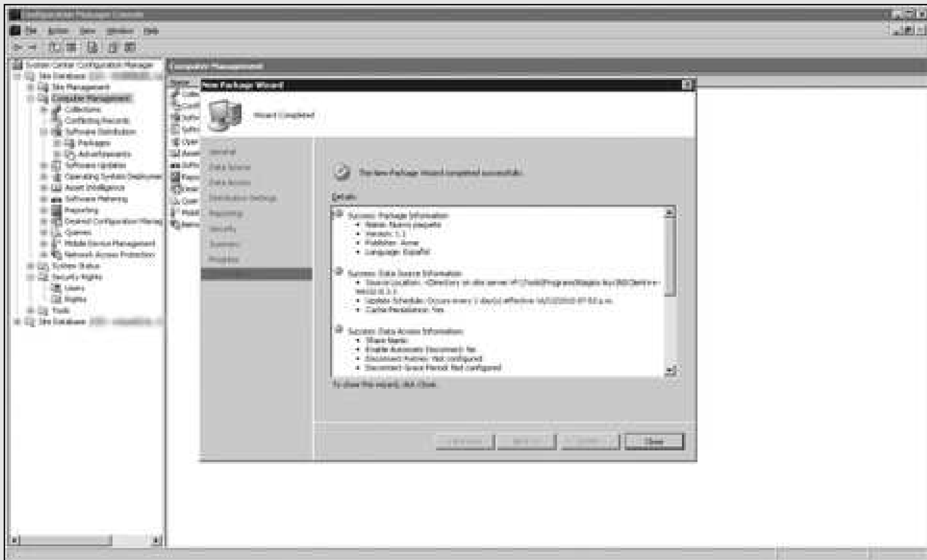
7 Al hacer clic sobre el botón llamado **Next**, deberá asegurarse de que la primera opción esté correctamente seleccionada. Luego, podrá oprimir el botón **Next** para continuar con el proceso.



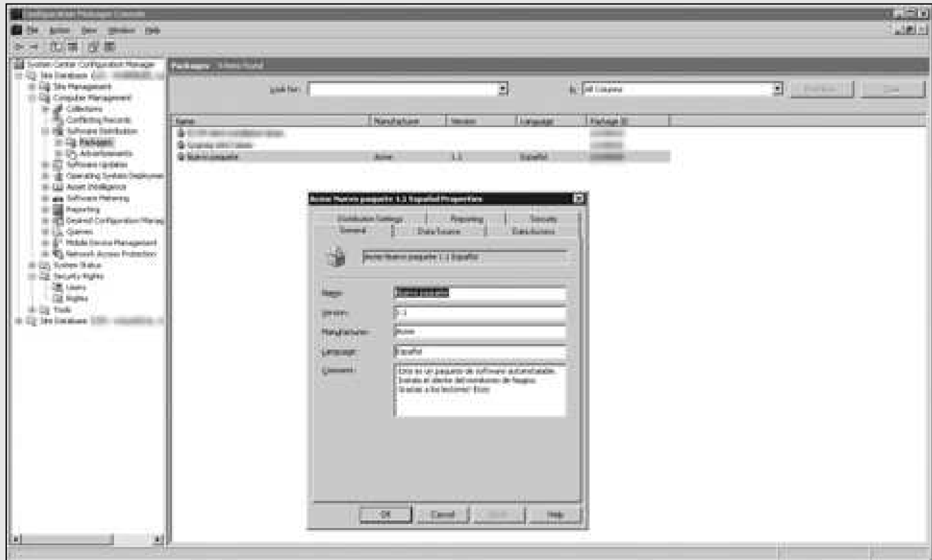
8 En este paso deberá seleccionar las opciones para los puntos de distribución correspondientes. En principio, puede elegir la prioridad y el protocolo de transmisión. Deje lo demás como está y presione **Next**.



9 Vea las opciones de **Reporting**; deje la primera seleccionada y presione el botón **Next**. Luego revise los detalles de seguridad, el resumen y oprima sobre **Finish** cuando haya terminado de crear el paquete.



10 Vaya hasta **Packages** otra vez, oprima **F5** y seleccione el paquete recién creado. Haga clic derecho y elija **Properties** para ver o modificar las opciones.



Luego de crear el paquete de software, será necesario que procedamos a repartirlo a los puntos de distribución para, luego, llevarlo a los equipos de la red correspondiente. A continuación, entregamos todos los detalles sobre este tema.

Distribución de un paquete de software

La distribución se realizará mediante los puntos de distribución (DP) que tengamos en nuestra infraestructura. Uno de ellos puede ser el servidor principal; luego, podemos elegir algún otro más. Los puntos de distribución se establecen al crear los paquetes, pero también pueden administrarse después desde sus propiedades. A los puntos que seleccionemos se sincronizarán los instaladores del software. Podemos poner los



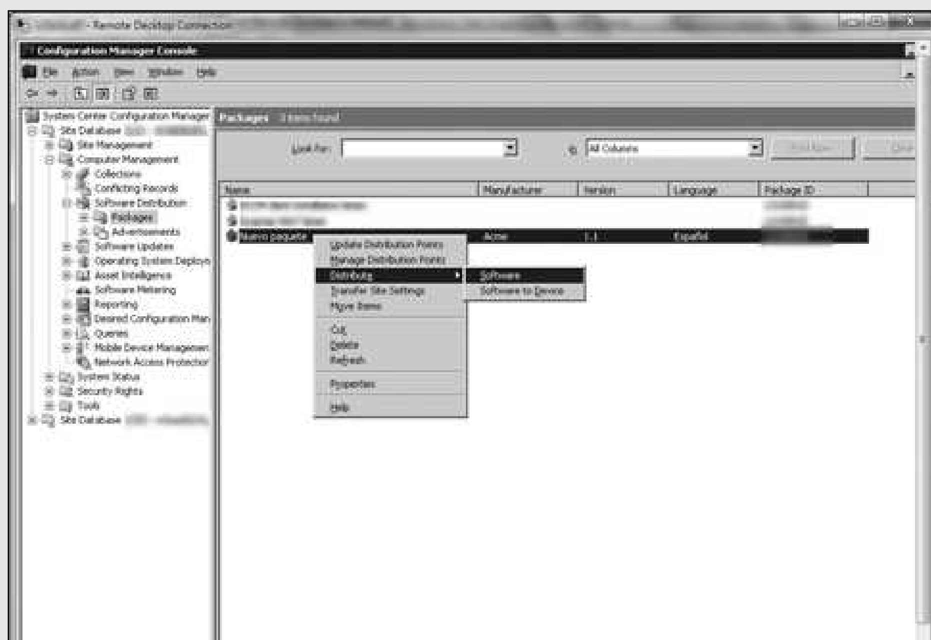
OTRA FORMA DE REPARTIR SOFTWARE

Otra manera de distribuir software en forma masiva es mediante el uso de las políticas de grupo (GPOS). El único inconveniente de esta práctica es que no tendremos un análisis del progreso de las instalaciones; no sabremos si el instalador se ejecutó correctamente o no. SCCM, sin dudas, es la mejor solución para realizar esta tarea.

que queramos, evitar alguno en particular o poner todos. Una vez configurado un punto de distribución en el armado del paquete, se generará la carpeta compartida con el mismo nombre para todos los puntos. Esto es de gran ayuda porque, algunas veces, ocurre que cierto software no se puede instalar porque le faltan archivos en su origen, en un punto de distribución en particular. Para subsanar estos conflictos, debemos buscar la carpeta en otro punto de distribución y copiar a mano otra vez los archivos, o actualizarlos desde las propiedades del paquete en cuestión. Ahora, veremos cómo distribuir un software a los puntos de distribución de forma práctica.

■ Distribuir un paquete de software a los DPs — PASO A PASO

1 Vaya hasta la opción denominada **Packages**, seleccione un paquete y haga clic derecho sobre él. Seleccione **Distribute/Software**.



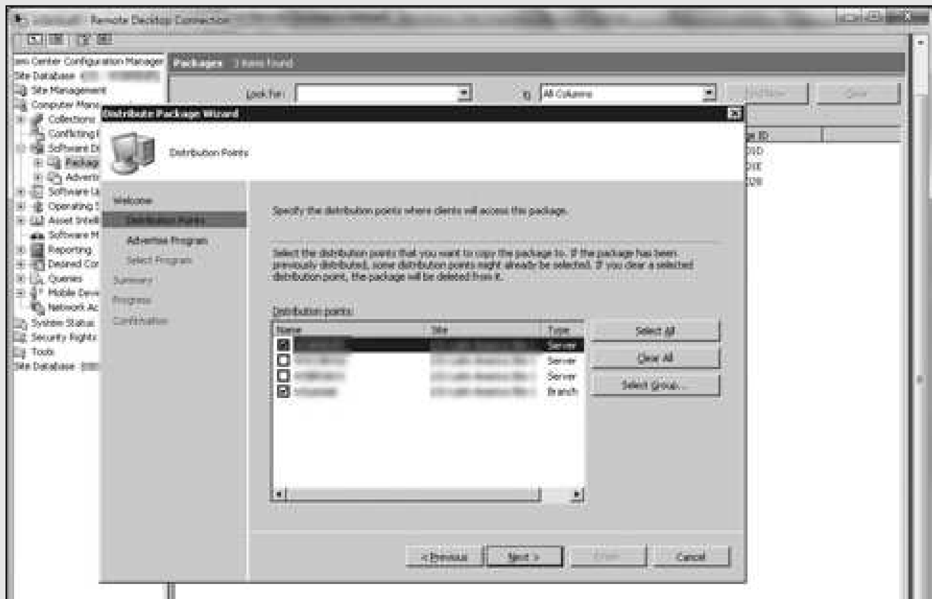
▶

✱ WINDOWS UPDATE

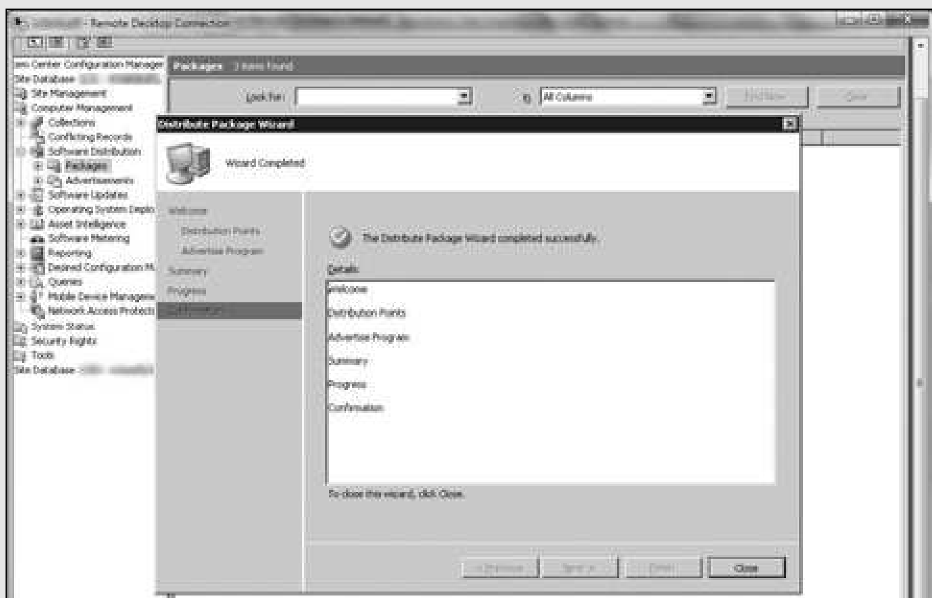
Los sistemas Windows se actualizan desde Internet gracias a esta herramienta que viene desde la versión 98. Ya en Vista, Windows 7 y 2008 se presenta como una aplicación exclusiva para esta tarea, de modo que no hace falta ingresar al sitio web. Estas actualizaciones no pueden permitirse, porque no sabemos cómo incidirán en nuestros sistemas; debemos probarlas antes.

▶

2 En la ventana emergente, oprima **Next** y seleccione los puntos de distribución a los cuales desea que llegue el paquete. Luego presione **Next**.

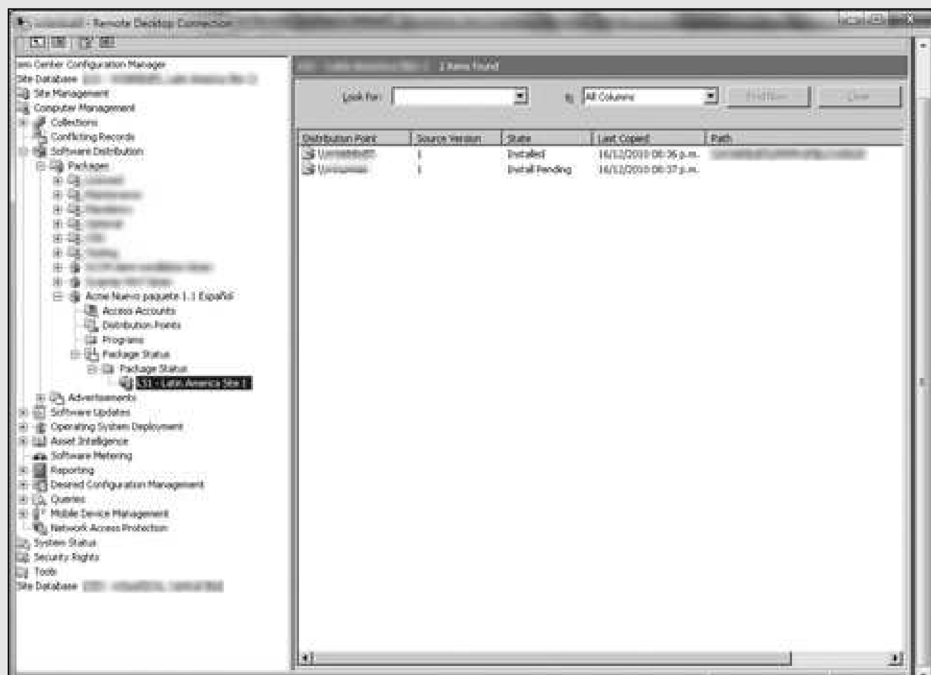


3 En las advertencias seleccione la opción llamada **No** y pulse el botón **Next**. Vea el resumen, oprima **Next** y, luego, **Finish**.



▶

► **4** En el paquete expanda las opciones y vaya hasta **Package Status/Package Status/Site Code elegido** para ver el progreso de la distribución.

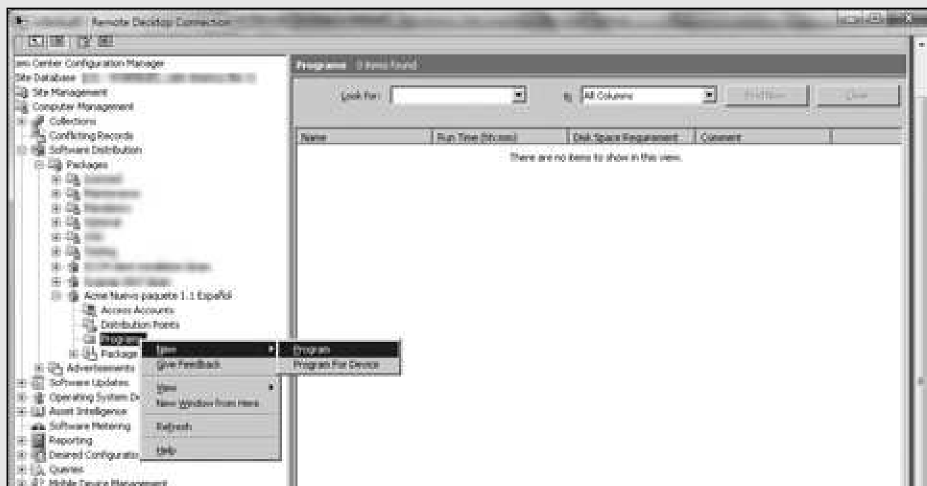


Si recordamos nuestro ejemplo en donde tenemos Argentina como site server, y las subsidiarias Brasil, Chile, Colombia y Ecuador, imaginemos que los puntos de distribución están protegidos, y los clientes de Ecuador sólo se conectan al punto de distribución de ese país. Si no queremos repartir un software determinado a Ecuador, evitamos colocar ese punto de distribución en las propiedades del paquete. Al colocar un punto de distribución, el paquete comenzará a copiarse. Veremos rápidamente cómo se crea una carpeta y, a continuación, cómo se copian los archivos a ella. En las propiedades del paquete, podremos ver su estado en cada DP. No bien figure en algún DP como instalado, estará disponible para ser bajado. La distribución no comienza a realizarse con la mera creación del paquete y la distribución a los DPs, sino que es necesario avisarles a los clientes que tienen un nuevo software para instalar.

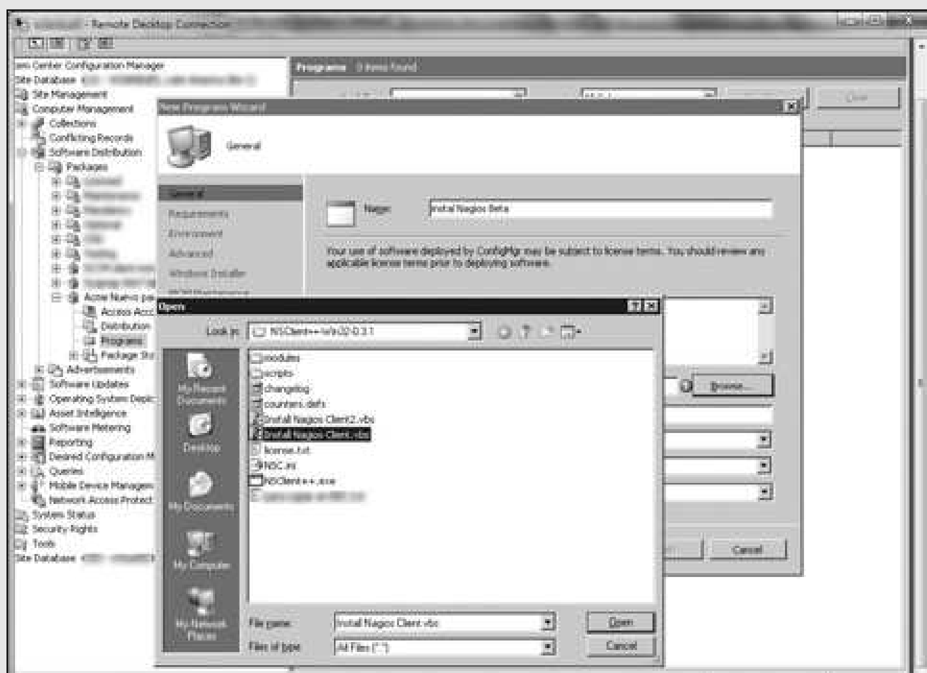
Para dar aviso a los clientes, el siguiente paso es asignar el programa a los clientes de alguna colección. Pero antes es necesario configurar un programa que se ejecutará para el paquete. De esta forma, le decimos al paquete que realice determinada acción una vez que se baje a algún equipo de la red. Podemos elegir un MSI o un script; a continuación, un paso a paso con los detalles.

Asignar un programa que se ejecutará en el paquete — PASO A PASO

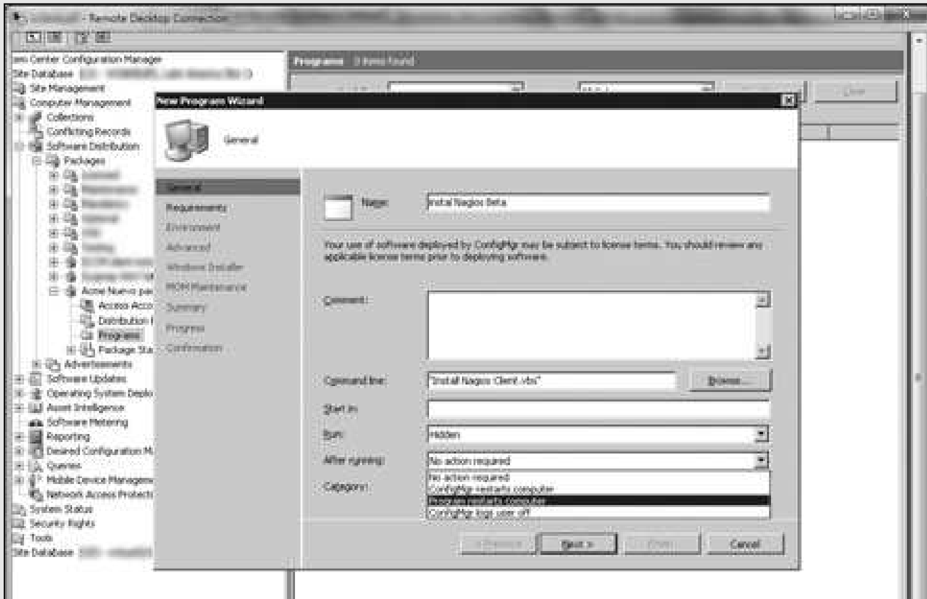
1 Diríjase hasta el paquete dentro de la carpeta **Packages**. Expanda las opciones y haga clic derecho en **Programs**. Seleccione **New/Program**.



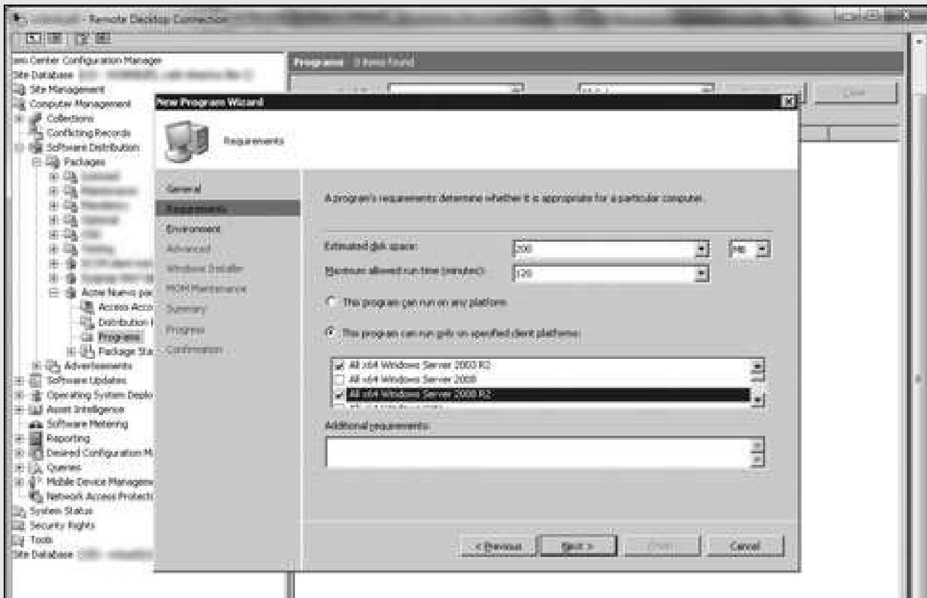
2 A continuación escriba un nombre y oprima sobre la opción **Browse** para seleccionar el script de la carpeta de instalación.



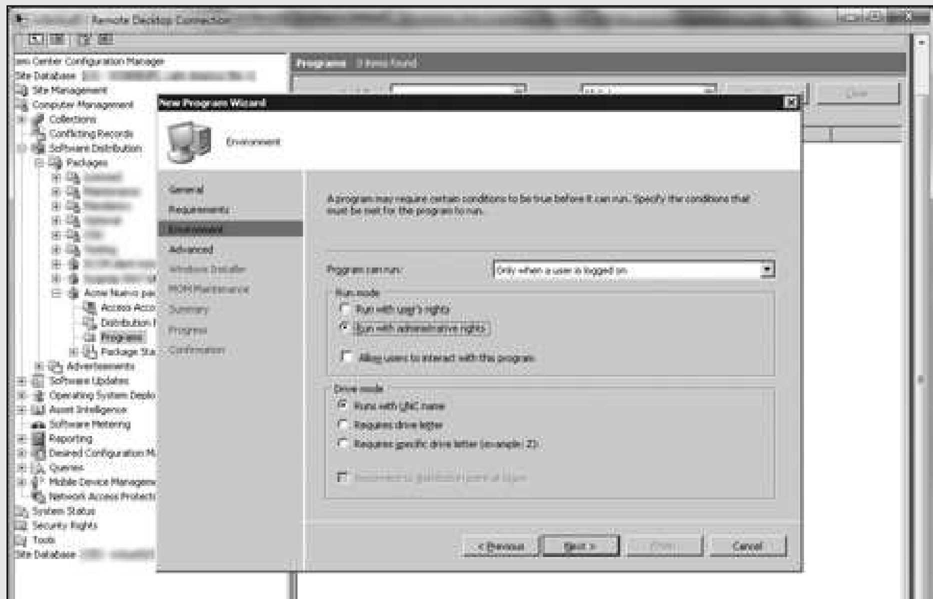
3 Seleccione el nivel de ejecución, las acciones a tomar luego de ejecutarse el instalador y ubique el programa en una categoría de paquetes si lo desea. Oprima **Next**.



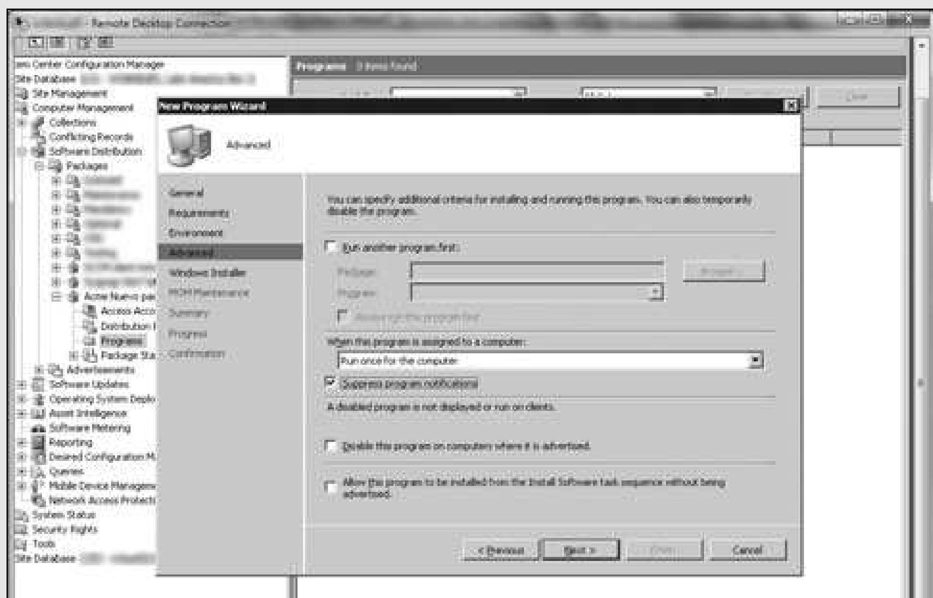
4 Ingrese el espacio en disco estimado, la cantidad máxima de minutos para la ejecución y el sistema operativo, si quiere restringir la instalación.



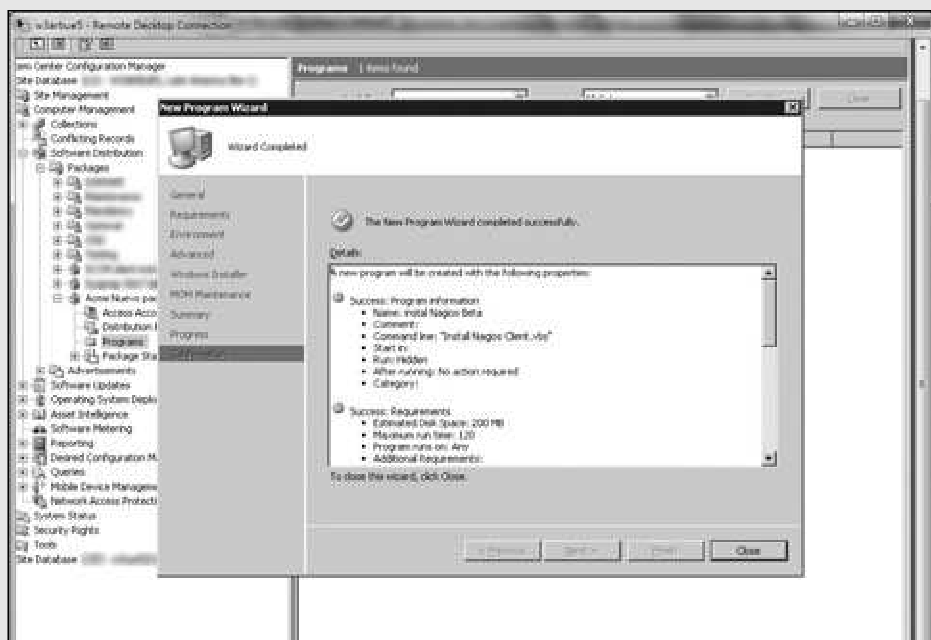
5 Seleccione las pretensiones de ejecución con respecto al login del usuario. Elija **Run with administrative rights** para que se instale con permisos de administrador.



6 En las opciones avanzadas presentadas, puede elegir repetir la instalación y, también, suprimir las notificaciones entregadas por el asistente.



7 En las opciones de **Windows Installer** oprima **Next**; en las opciones de **Microsoft Operations Manager** (MOM) haga lo mismo, vea el resumen y oprima **Finish**.



Nuestra tarea no termina todavía: debemos realizar una advertencia (advertise) del paquete de software a alguna colección que queremos que se instale. Podemos sólo advertir dicho paquete para que aparezca en un listado de software disponible, o seleccionar la opción de instalar en las mismas opciones de creación del paquete. La instalación (assignment) puede programarse no bien esté disponible o en alguna fecha en particular. Podemos elegir dar aviso al usuario o, directamente, instalarlo. En caso de avisar, podemos dar un rango de fecha en que el usuario puede hacerlo o instalarlo en una fecha de vencimiento. Tenemos la posibilidad de forzar el reinicio del equipo una vez instalado o dejar la decisión al usuario.

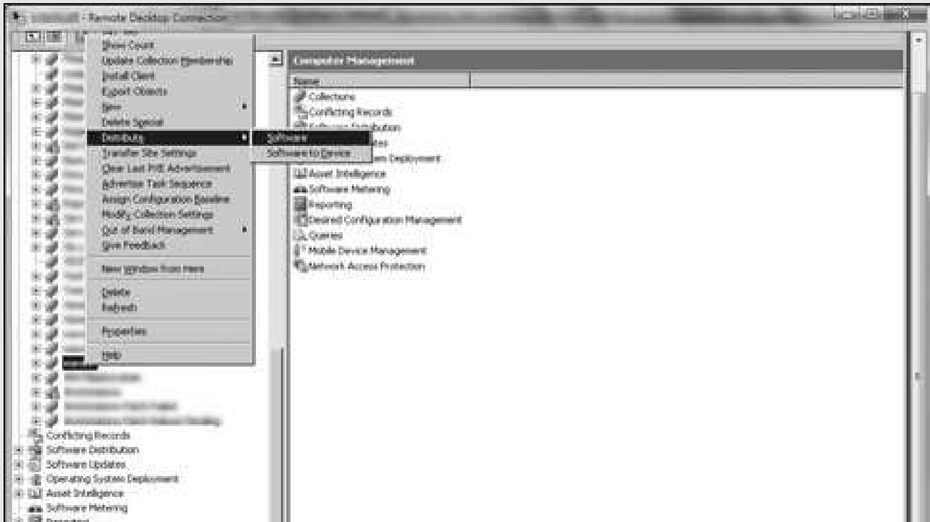


PERMISOS A LA CONSOLA MMC DE SCCM

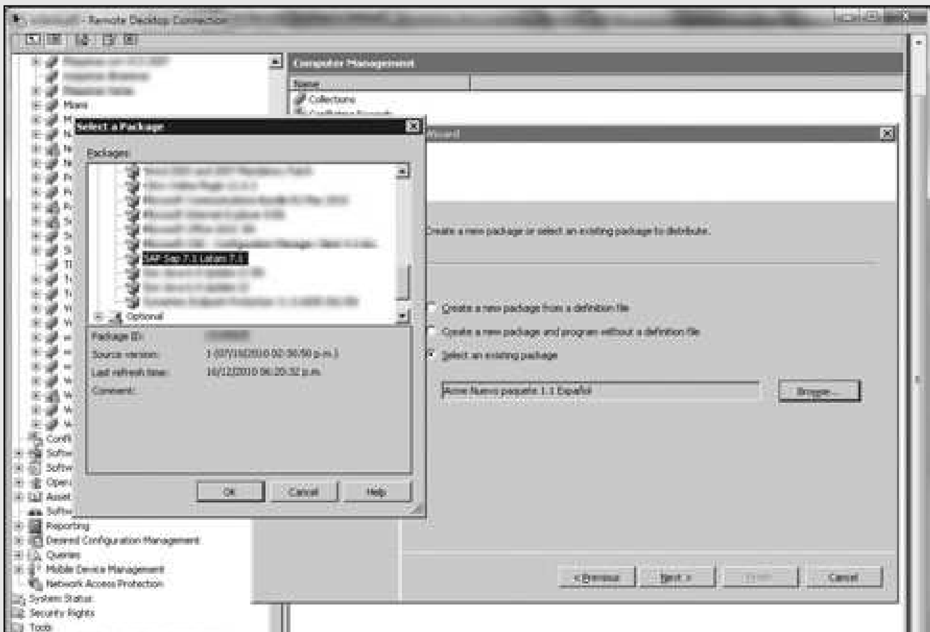
Es necesario saber que más allá de los permisos que podemos administrar para los reportes de SCCM, también es posible otorgar permisos a los usuarios para conectarse a la consola de SCCM y hacer algunas tareas en ella. Podríamos dar permisos de modificar cierta colección o dar acceso sólo a la implementación de parches o software.

■ Distribuir y advertir un paquete a una colección — PASO A PASO

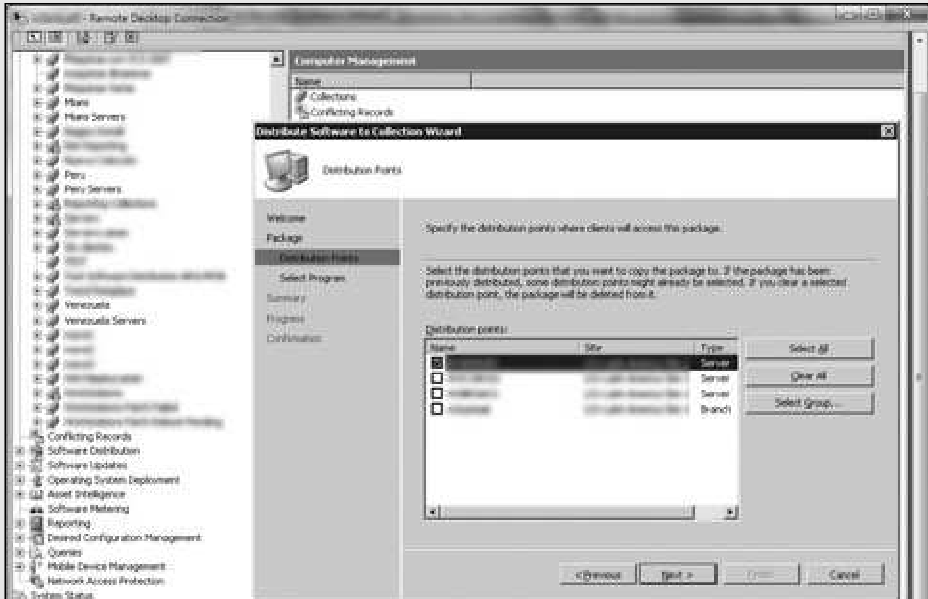
1 Vaya a la colección objetivo, haga clic derecho y seleccione **Distribute/Software**. Esto abrirá un ayudante. Lea el mensaje y oprima **Next**.



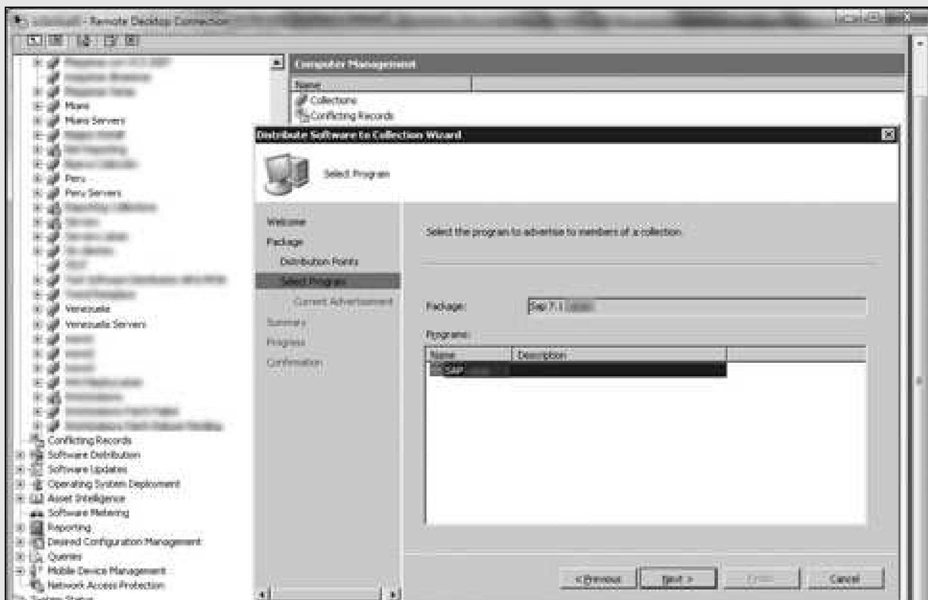
2 Elija **Select an existing package** y oprima en **Browse**. En el listado que aparece, elija el paquete que quiere distribuir.



3 Seleccione los puntos de distribución a los cuales los clientes podrán acceder para bajar el paquete e instalarlo.

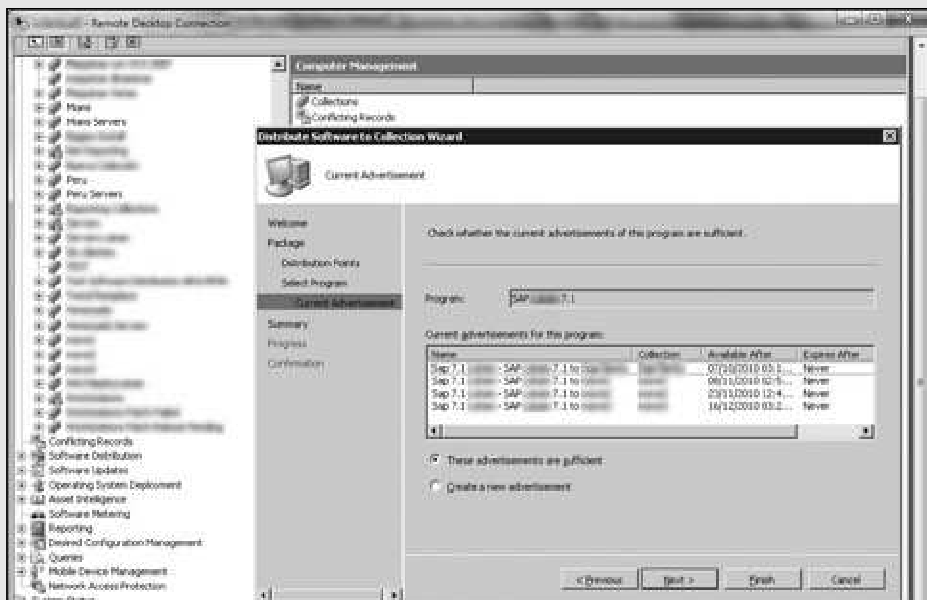


4 Elija uno de los programas que contenga el paquete. Deberá recordar que los programas fueron creados anteriormente.

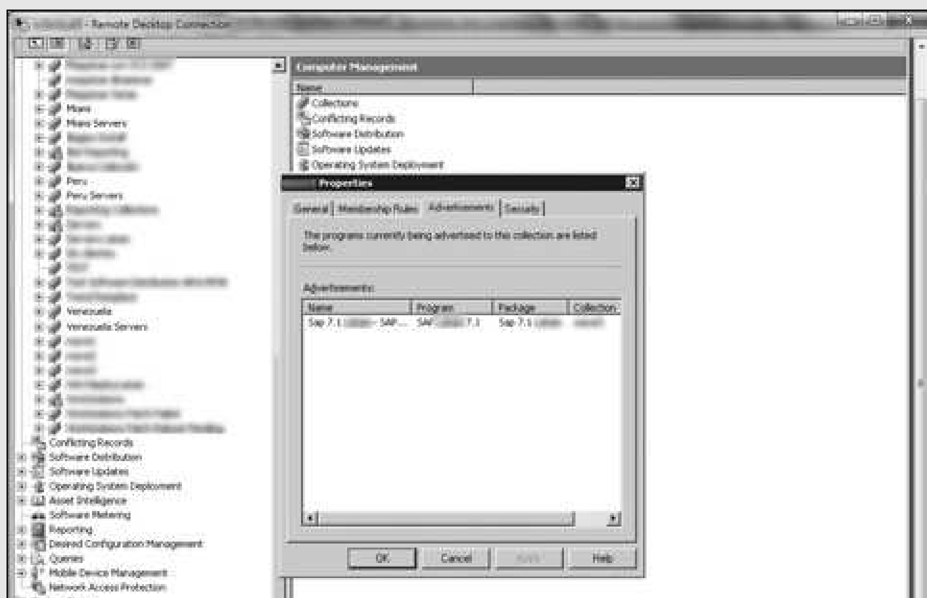


▶

5 Esto genera una advertencia de un nuevo programa a todos los objetos de la colección. Si cree que no es suficiente, puede crear otra advertencia.



6 Vea el resumen, el progreso de la creación y oprima **Finish**. En las propiedades de la colección debe figurar esta nueva advertencia, dentro de la solapa **Advertisements**.



Luego de estos simples pasos, el o los paquetes que distribuyamos comenzarán a advertirse a los clientes. Podemos programar la instalación automática si vamos hasta: **Site Database/Computer Management/Software Distribution/Advertisement** y elegimos la nueva advertencia creada. Realizamos un clic derecho y escogemos **Properties**. Allí podemos configurar que se instale no bien sea posible, o en una fecha y un horario determinados. Generalmente, se programan días posteriores de instalación a la fecha de distribución. De esta forma, el paquete es distribuido a todos los clientes, y el día de la fecha de instalación comienzan a instalarse todos juntos.

Seguimiento de una distribución

Una vez que se haya distribuido el software a los DPs y la advertencia del nuevo software se haya creado, los clientes de la colección a la que se distribuyó el paquete irán a buscar el DP más próximo de los habilitados. Cuando el cliente se contacte con su DP, comenzará a bajar el paquete localmente para instalar. Puede ser que no necesitemos bajarlo y ejecutemos el instalador desde el servidor, pero esta práctica no se utiliza y no es recomendable, ya que podemos consumir los recursos del servidor muy fácilmente, con pocos clientes conectados. Entonces, el cliente baja el instalador a una carpeta que ya nombramos, la carpeta caché ubicada en **C:\Windows\System32\CCM\Cache** o, para sistemas 64 bits, **C:\Windows\SysWOW64\CCM\Cache**. Cuando termina de bajar el paquete, ejecuta el programa que éste indica en sus propiedades. De esta manera, instala el software y luego informa la situación al Management Point. Entonces, desde la consola, podemos ir a Site System Status y, allí, pararnos sobre Advertisement Status, donde veremos todas las advertencias de software que hemos generado. Al hacer clic en cada una, se nos dará información de estado, equipos que recibieron el paquete, equipos que pudieron ejecutarlo, equipos que fallaron, y otros datos más. Rápidamente, observaremos el avance de la instalación y descubriremos fallas generales en caso de ocurrencia. Podemos distinguir los equipos en que no se instalaron, para solucionarlo rápidamente y cumplir con el 100% del objetivo principal.

Veremos los equipos en los que haya fallado la instalación si en la ubicación que antes marcamos realizamos clic derecho sobre la advertencia del paquete y elegimos **View Messages**. La instalación de algún software puede fallar en algunas ocasiones si



ALTIRIS

Es una herramienta competidora de SCCM adquirida por la empresa Symantec alrededor del año 2007 para completar los productos de seguridad que ofrece esta compañía. Altiris es compatible también con sistemas Mac OS, Linux, Novell Suse y Red Hat. Para empresas grandes, es un gran complemento de SCCM por abarcar todos los sistemas.

la sincronización del paquete falló por algún motivo. Podemos encontrar fallas en varios clientes, y en otros no. Esto quiere decir que hay un DP que está distribuyendo el paquete de forma errónea. Entonces, analizamos los equipos con errores y encontraremos el punto en común. Si fuese así, y descubrimos el DP que falla, borramos la carpeta del paquete con problemas y, desde el site, entramos en las propiedades del paquete y volvemos a sincronizarlo. Esta acción creará otra vez la carpeta y volverá a copiar los archivos. Un error muy común que sucede sin darnos cuenta es que los discos se llenan, sobre todo, en DPs que no están exclusivamente para el uso de SCCM. Como falta espacio en disco, el paquete nunca termina de copiarse bien. En DPs branch puede suceder que falle por algún sector dañado de un disco; en ese caso, el sistema operativo y SCCM creen que se tienen las versiones correctas, cuando, en realidad, el archivo está dañado. Entonces, con borrar y volver a copiar no alcanzará para solucionar el problema: debemos reparar el disco antes de volver a sincronizar. El mundo de SCCM es muy amplio y está repleto de estos posibles errores, que aprenderemos a manejar con la experiencia.

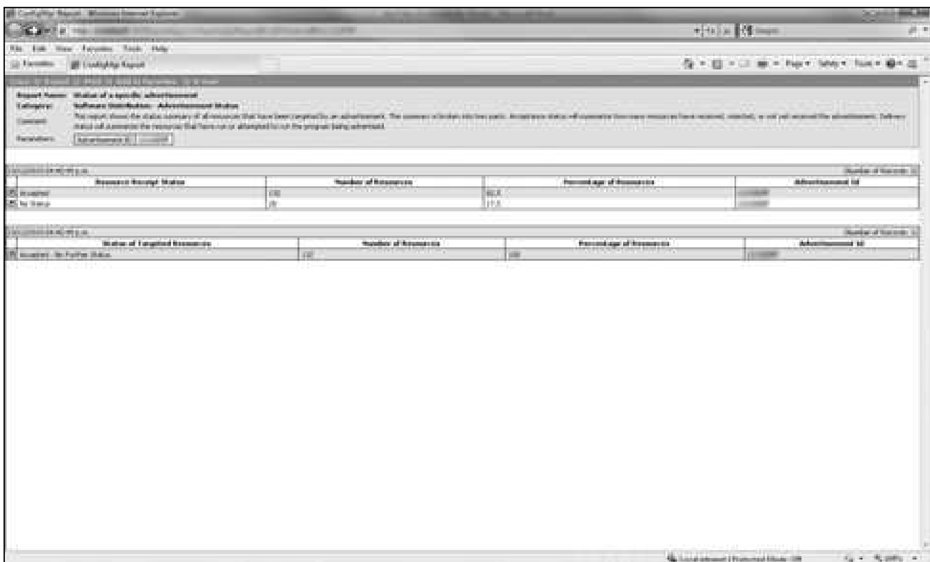


Figura 3. *Como un adelanto a los reportes, podemos ver aquí el estado de instalación de un paquete de software.*



LEY SARBANES-OXLEY

También denominada SOX, SarbOx o SOA, es una ley que nació en EE.UU. para monitorear empresas que cotizan en Bolsa. La ley protege al inversor asegurando que no haya fraudes ni riesgos de bancarrota. Sin dudas, los reportes de SCCM son una herramienta clave para el área de auditoría interna que requiere esta ley para las grandes empresas.

CREACIÓN DE PARCHES

Como dijimos antes, la distribución de los parches juega un papel esencial en la continuidad del negocio, y SCCM viene a ayudarnos en esta tarea. WSUS es una herramienta muy difundida y utilizada, que tenía su propia autonomía hace unos años, y que ahora Microsoft incluye en SCCM. Éste toma la administración de WSUS para brindarnos el mayor aprovechamiento posible de sus capacidades. Podremos formar paquetes de parches, probarlos y, luego, distribuirlos en forma masiva, para así evitar la instalación inadecuada de cualquier actualización automática o manual de Internet que afecte a nuestra empresa.

Búsqueda de nuevos parches

Todos los meses, Microsoft publica una serie de boletines con parches de seguridad. En general, salen a fines de mes, salvo en casos excepcionales de extrema urgencia, cuando se publican no bien están disponibles. Entonces, nuestra tarea será crear un paquete de actualizaciones una vez por mes, excepto cuando tengamos que solucionar una falla crítica. Las empresas suelen dividir el armado de paquetes entre parches de máquinas de escritorio y parches de servidores. Esto es porque la administración de dichos equipos pertenece a departamentos separados, que deben llevar sus propios análisis, administración y mantenimiento. No tiene sentido tampoco crear grandes paquetes que contengan todos los parches de un mes entero para ambas plataformas. Nosotros nos centraremos, entonces, en los parches para servidores, que es lo que nos compete. Veremos más adelante, en este mismo capítulo, un paso a paso que contiene todas las indicaciones correspondientes, pero a continuación analizaremos los detalles relacionados con el proceso.

El armado de paquetes de parches comienza con su búsqueda. Para este fin, utilizamos reglas de búsquedas en la consola SCCM; puede ser alguna genérica o la nuestra propia. Estas reglas de búsqueda se encuentran en: **Site Database/Computer Management/Software Updates/Update Repository/Search Folders**.

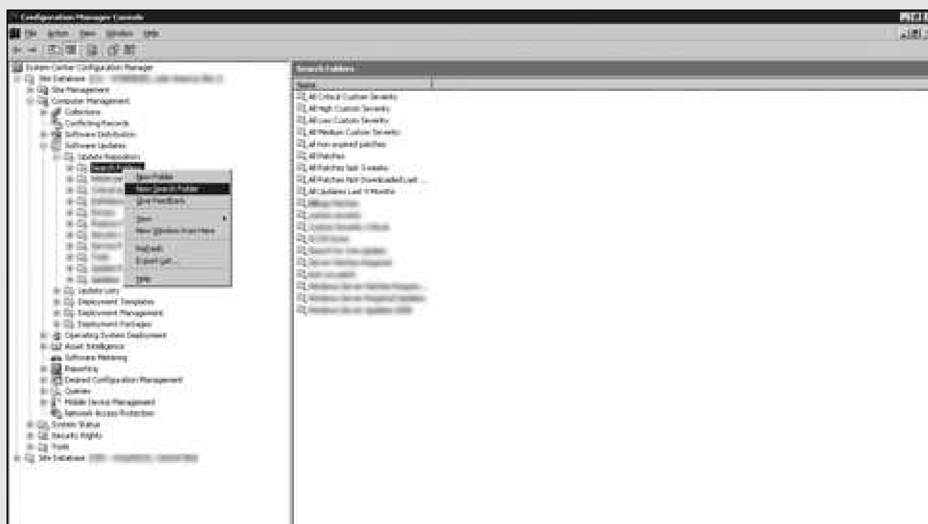
Podemos tener varias reglas que se adapten a nuestro negocio, pero con tener una para máquinas de escritorio y otra para servidores, basta y sobra. Estas reglas se definen como **Search Folders** (carpetas de búsqueda).

Cada una de las carpetas de búsqueda tiene características especiales para elegir productos, criticidad de los parches y tipos de parches, entre otras opciones importantes. En nuestra regla creada, SCCM se conectará con Windows Update para traernos los últimos parches publicados que cumplan nuestras reglas. Debemos tener en cuenta que con esa regla, podremos proceder a elegir los parches necesarios para armar un paquete de actualizaciones, que llamaremos Update List (lista de actualizaciones). A continuación, veremos cómo armar una lista de actualizaciones con las indicaciones detalladas para cada parte del proceso.

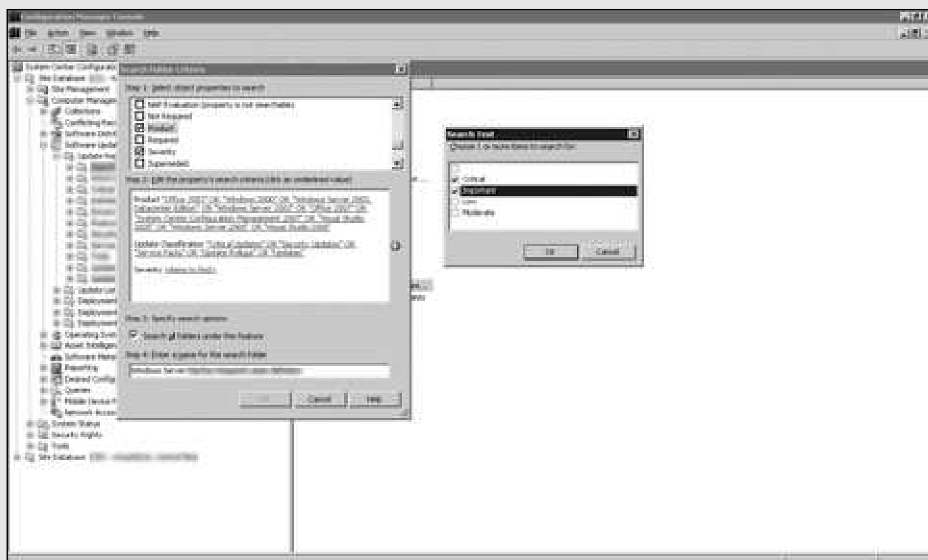
Armar un Update List

PASO A PASO

1 Vaya a la consola SCCM y diríjase a **Site Database/Computer Management/Software Updates/Update Repository/Search Folders**. Allí, haga clic derecho y seleccione **New Search Folder**, coloque un nombre e ingrese en las propiedades.

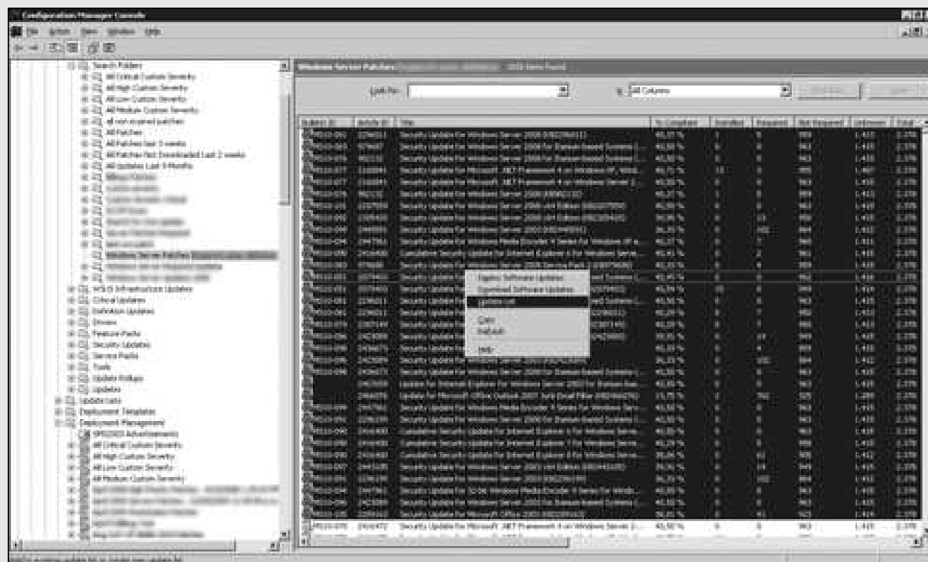


2 Allí puede elegir distintos objetos con diferentes propiedades. Ingrese a **Update Clasification**, por ejemplo, y seleccione la severidad de las actualizaciones. Complete y oprima en **OK** para cerrar las propiedades.

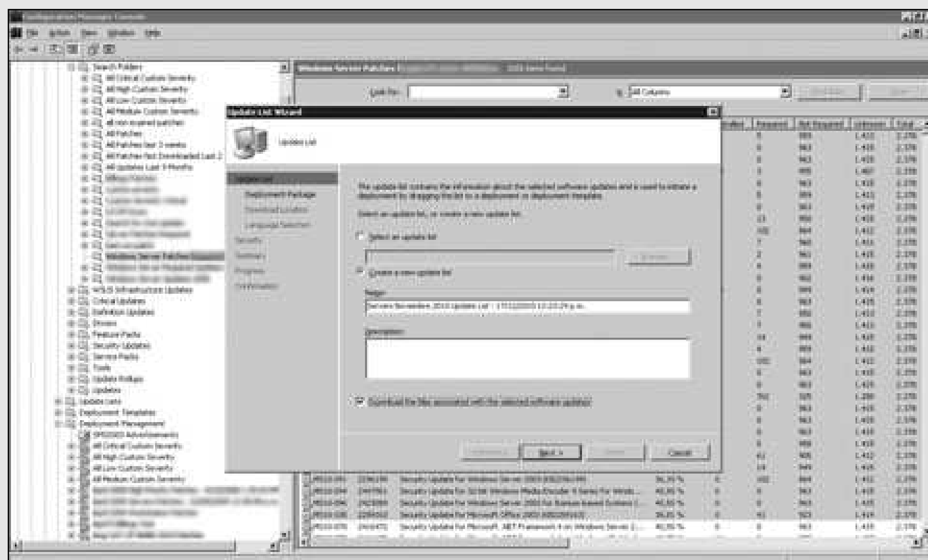


▶

3 Para continuar, ingrese a la carpeta de búsqueda que ha sido creada y seleccione las actualizaciones que formarán parte de la lista correspondiente. Haga clic con el botón derecho del mouse y elija la opción **Update List**.

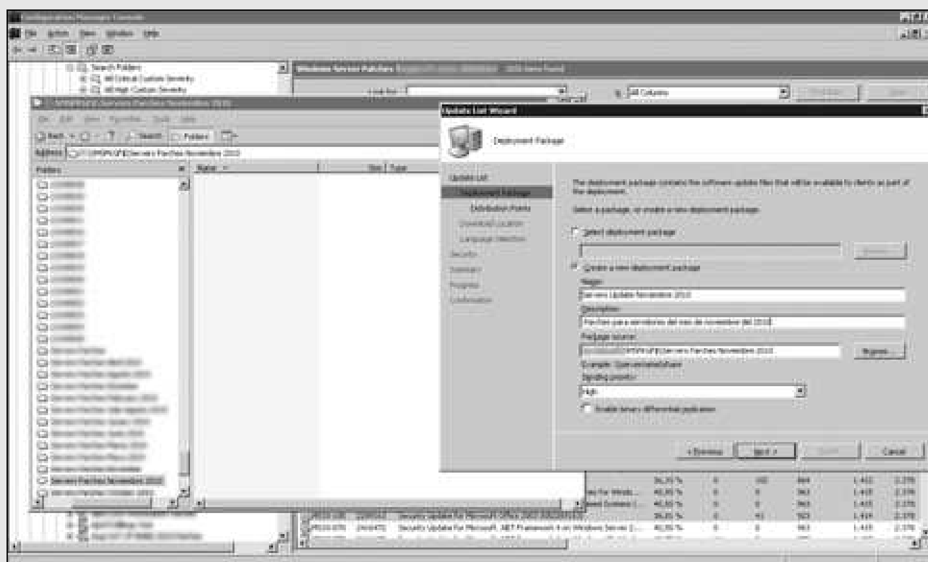


4 En la ventana emergente escoja la opción denominada **Create a new update list**. Escriba un nombre para el listado, seleccione **Download the files associated with the selected software updates** y pulse sobre **Next**.

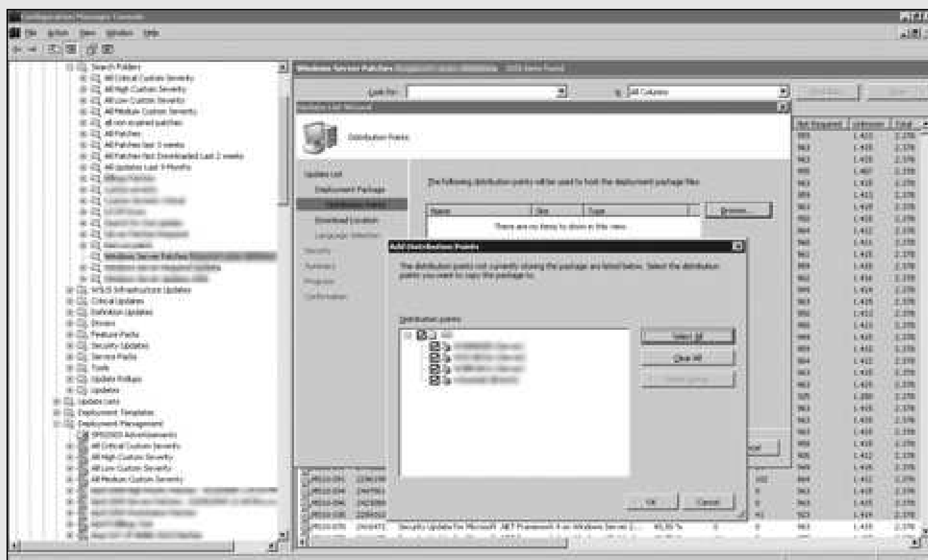


▶

5 Deberá tener en cuenta que en el mismo ayudante se crea la implementación hacia los puntos de distribución. Seleccione **Create a new deployment package**, escriba un nombre y una descripción, seleccione el origen de los paquetes (una carpeta compartida local) y oprima **Next**.

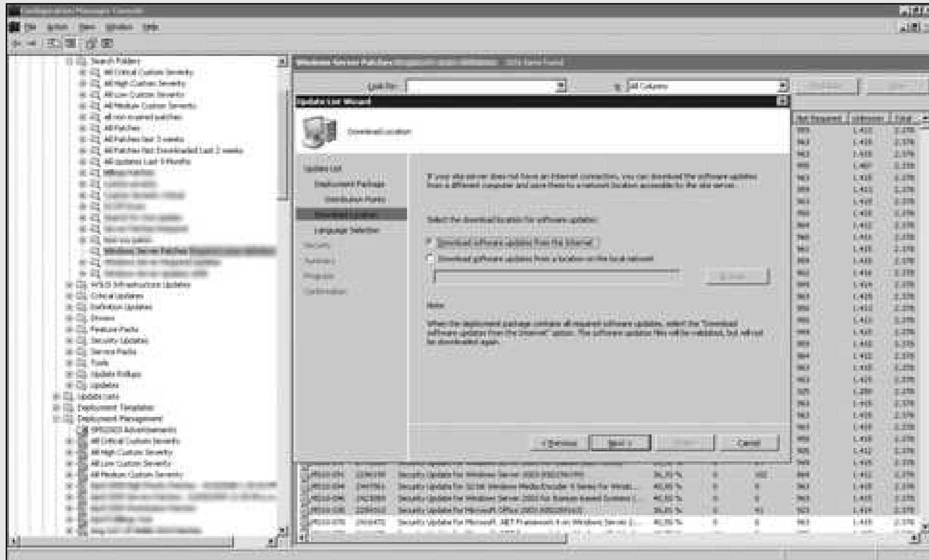


6 Elija los puntos de distribución a los cuales se bajarán las actualizaciones. Oprima **Browse** y seleccione los que crea necesarios. Presione **OK** y, luego, **Next**.

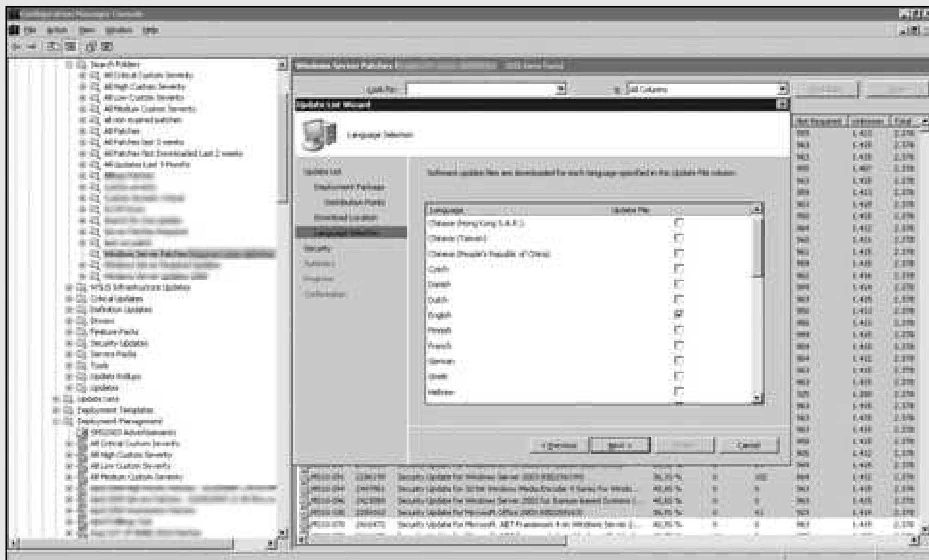


▶

7 Antes de continuar asegúrese de que la opción denominada **Download software updates from Internet** se encuentre seleccionada; luego de comprobarlo deberá hacer clic sobre el botón **Next**.

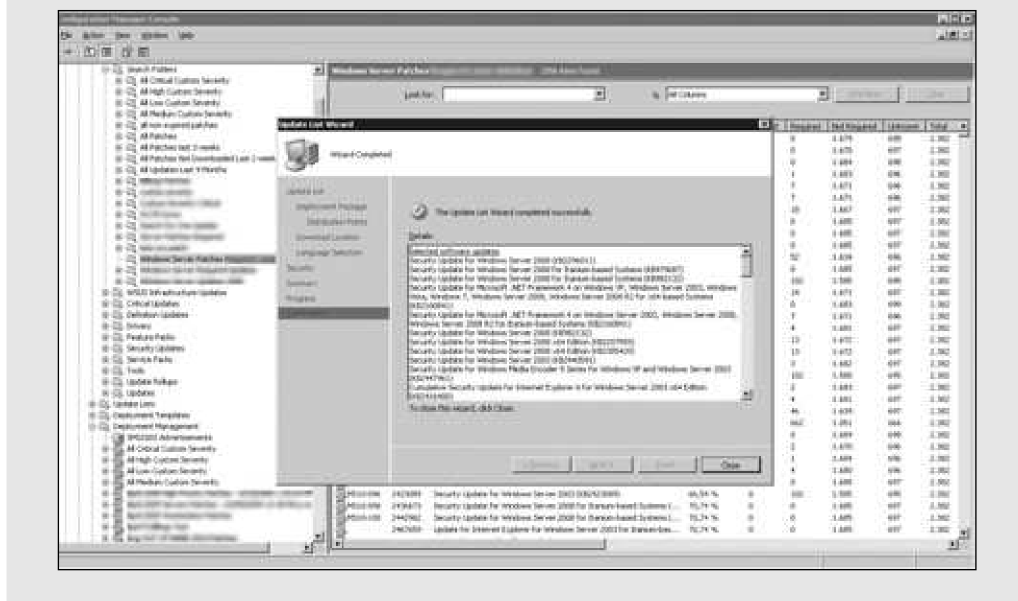


8 A continuación, deberá proceder a elegir cada uno de los lenguajes que corresponden a sus equipos en la red; de esta forma se asegurará de que se bajen e instalen sólo las versiones de actualización correctas.



▶

9 Vea las opciones de seguridad, el resumen y oprima **Finish**.



Debemos tener cuidado de no bajar parches de más, ya que ocupan demasiado espacio en los puntos de distribución si no se usan. No tiene ningún sentido guardar parches de sistemas viejos. Por ejemplo, Microsoft ya no da soporte para Windows 2000; entonces, lo correcto sería analizar los Windows 2000 de la empresa, tratar de migrarlos si es posible o instalarles las últimas actualizaciones. De esta forma, ya podremos borrar de nuestros puntos de distribución todos los parches que corresponden a esta versión de sistema operativo. Obviamente, suponemos que no volveremos a instalar Windows 2000 nunca más. Esto debe establecerse como una política de trabajo, y podemos proponerla en cualquier momento como una muy buena práctica.
Casi finalizando el ayudante para armar la lista, veremos que empieza a bajar los parches al servidor; cuando termina, el ayudante finaliza y avisa que todo está



BLACK HAT

Nació en 1997 y es la conferencia de seguridad más importante del mundo. En ella se reúnen los hackers y empresas de seguridad para dar a conocer vulnerabilidades en todo tipo de sistemas. Microsoft comenzó a participar en ella al salir Windows Vista y, actualmente, espera ansiosa las fechas para sacar nuevos parches para sus sistemas operativos. **www.blackhat.com**.

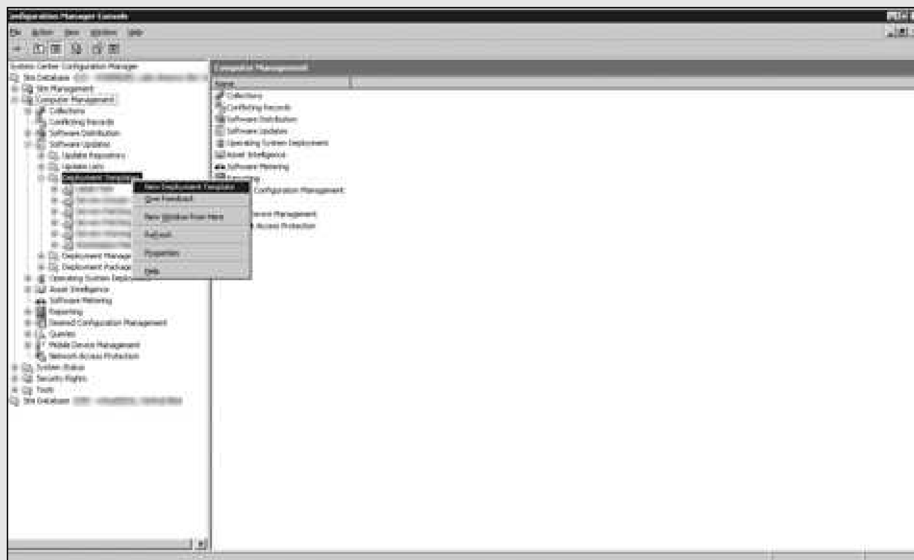
terminado. Entonces, podremos ver el Update List creado en: **Site Database/Computer Management/Software Updates/Update Lists**.
Como siguientes pasos, definiremos templates (plantillas) a los cuales se les configurará una colección por defecto, que es la que se usará para armar el paquete de implementación que generaremos más adelante.

Templates de distribución

Luego de armar el Update List, tenemos que definir los templates, que serán usados para el deployment (despliegue de los parches), es decir, la distribución propiamente dicha. Los templates se definen para una colección en especial. Lo conveniente es tener templates de pruebas y otros que abarquen a todos los dispositivos. Entonces, habrá un template que llamaremos Servers Test y otro que llamaremos Servers. Los nombres pueden variar, son sólo a título de ejemplo. Los templates se definen en la siguiente ubicación: **Site Database/Computer Management/Software Updates/ Deplyment Templates**. Allí tendremos un listado de los que hayamos definido.
Sabemos que se trata de un procedimiento muy sencillo, por lo tanto nos tomará muy poco tiempo completarlo, entregamos más detalles en el siguiente **Paso a paso**.

Cómo armar un template — PASO A PASO

1 Abra la consola, diríjase a **Site Database/Computer Management/Software Updates/Deployment Templates** y haga clic derecho en esa carpeta. Seleccione **New Deployment Template**.



▶

2 Escriba un nombre y una descripción, y oprima **Next**. Seleccione una colección de la lista, que será la representante del template, oprimiendo el botón **Browse**. Haga clic en **Next**.



3 Elija la opción **Allow display notifications on clients** para que los usuarios vean cuando se les instalan las actualizaciones. En caso contrario, elija **Suppress display notifications on clients**. Deje marcada la opción **UTC** y elija una duración de las notificaciones de los parches. Oprima **Next**.



▶

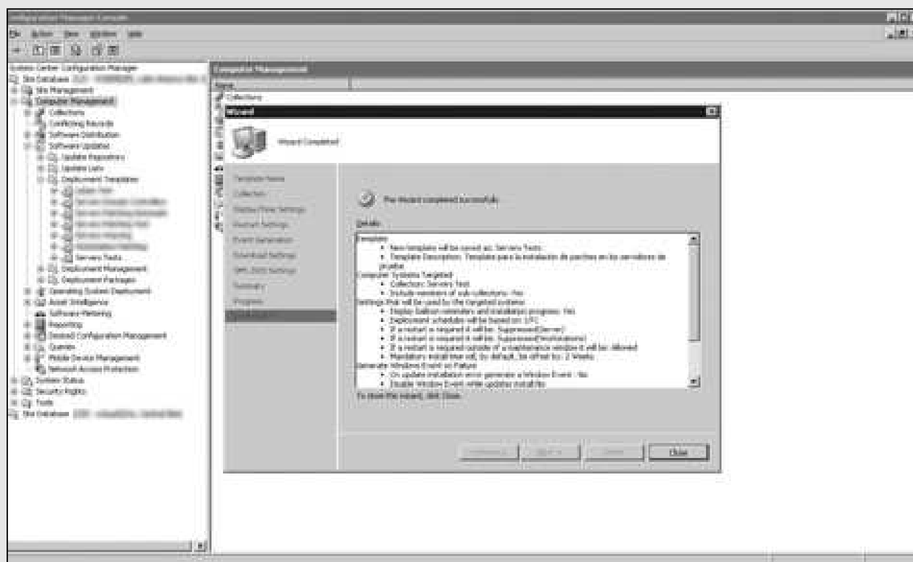
4 Marque las opciones **Servers** y **Workstations** para evitar que los equipos se reinicien si alguna actualización así lo requiere. Luego, haga clic en **Next**.



5 Deje las opciones en blanco y oprima **Next**. Después, elija **Download software updates from distribution point and install** si quiere que las actualizaciones se instalen una vez que se hayan bajado, y **Do not install software updates** para evitar que los clientes se conecten a puntos de distribución no adecuados.



► 6 Deje la opción en blanco y oprima **Next**. Vea el resumen, presione **Next** para ejecutar el procedimiento y, por último, en **Finish** para terminar.



El armado del template define una colección, opciones de reinicio para los equipos, tanto para máquinas de escritorio como para servidores. También indica si se suprimen o no las notificaciones a los usuarios de las actualizaciones por instalar. Un punto muy importante es que define si bajamos los parches en los servidores y los instalamos automáticamente, o si sólo los bajamos. El uso correcto de estos templates nos permitirá, por ejemplo, armar un escalonamiento de instalación de parches para hacer un mejor seguimiento. Este escalonamiento puede hacerse si tenemos tres templates, por ejemplo, en vez de uno. Esto evitará fallas graves de la siguiente forma. Lo que debemos plantear es una colección de pruebas, donde colocaremos un servidor representante de cada tecnología. Con esta colección creamos un template de pruebas. Luego, dejando los servidores críticos para el final, hacemos una colección de varios servidores más; es decir, un mayor número de servidores a los cuales podemos instalarles los parches automáticamente. Armamos un template intermedio. Por último, con una colección donde figuren todos los servidores anteriores más los críticos, armamos un template crítico. Con estos tres, podemos ir dando avance a las instalaciones de parches haciendo los testeos correspondientes. El template se define en el paquete de distribución. Entonces, en cuanto lo armamos, ponemos el template de pruebas. Lo dejamos una o dos semanas y, luego, colocamos el template intermedio. Si no tuvimos errores ni reclamos de fallas, recién a las tres o cuatro semanas, colocamos el template de críticos donde se instalará los parches a

todos los servidores de la empresa. Esta práctica permite ir instalando los parches en los servidores con un mayor control y probándolos antes de instalarlos en los servidores Exchange o Domain Controllers, por ejemplo.

Distribución de parches

Para comenzar la distribución de parches, hace falta crear el deployment (implementación), lo cual puede hacerse a partir de un Update List, que contiene el listado de parches. El deployment incluirá los datos del Update List y los enlazará con un template habilitando opciones de calendario para las instalaciones. El deployment hará lo mismo que una advertencia de software: les indicará a los clientes de la colección objetivo que tienen actualizaciones para instalar. Esta acción la realizará no bien se cree. Los clientes verán un aviso en la barra de tareas, similar al de Windows Update de Microsoft, pero de SCCM. Esto desplegará un listado con los parches y se comenzarán a instalar en el equipo una vez que el usuario lo apruebe.

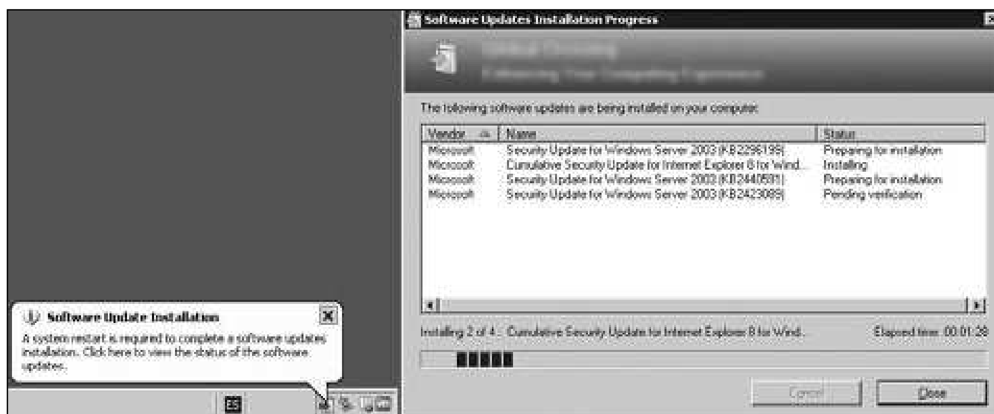


Figura 4. *En esta ventana podemos ver parte del proceso de instalación, la tarea completa no se prolongará por mucho tiempo.*

En caso de que tengan la opción automática, el usuario no tendrá que intervenir y, luego, se le mostrará un aviso de reinicio en el equipo. En la creación del Update



CATEGORÍAS DE SOFTWARE

Es importante tener en cuenta que es una gran idea categorizar el software que distribuimos a los equipos que corresponden a nuestra empresa; así, el usuario podría elegir entre software obligatorio, opcional o de pruebas, por ejemplo. De esta forma, damos también a conocer al usuario sus posibilidades y obligaciones.

List se definen los puntos de distribución a donde se copiarán las actualizaciones. Debemos tener en cuenta que las copias se realizarán de modo normal, es decir, sin utilizar BITS. Después de este procedimiento, cada uno de los clientes, dependiendo del punto de distribución que ha sido asignado en forma anticipada por el administrador, irán a buscar las actualizaciones a las carpetas correspondientes a cada uno. Aquí sí la bajada de los parches se realiza con BITS; de esta forma no se interfiere con el uso cotidiano de la máquina.
A continuación, podremos ver una descripción que nos ayudará a armar una implementación de parches para nuestra empresa.

■ Armar un deploy de parches — PASO A PASO

1 En la consola de SCCM, deberá dirigirse hasta la sección **Update Lists** y, en la lista de actualizaciones que quiera implementar, haga clic con el botón derecho del mouse y seleccione **Deploy Software Updates**.

►

{ } RESPONSABILIDAD DE LAS PRUEBAS

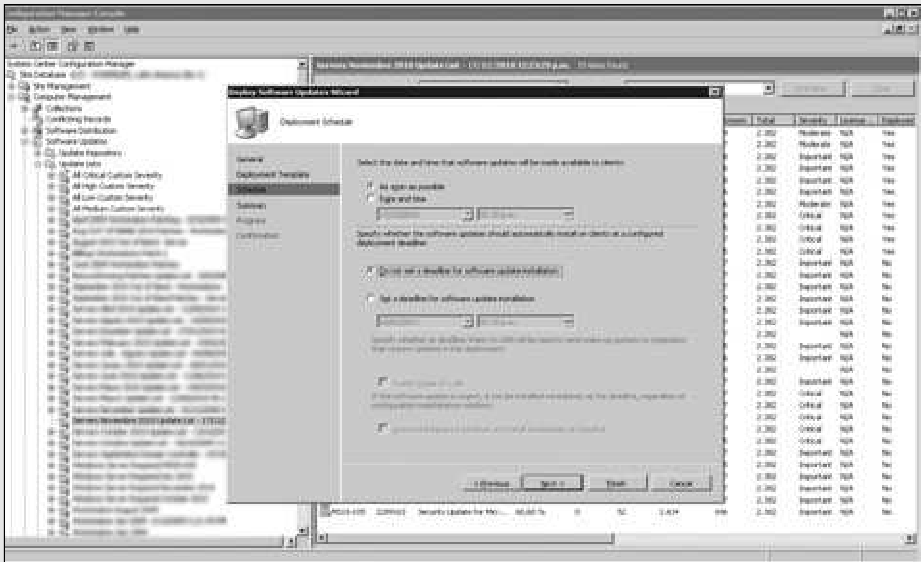
Debemos tener en cuenta que la responsabilidad de las pruebas de los parches es tanto nuestra como de los encargados de los servicios que corren en los servidores. Se deben establecer comunicaciones para ver el progreso de las pruebas y ejecuciones normales de todos los sistemas. Es importante asegurarnos de que no haya errores.

▶

2 Escriba un nombre y una descripción, oprima **Next**, elija el template y pulse **Next**.



3 Elija en qué fecha y horario los parches estarán habilitados para los clientes; más abajo, elija cuándo se deben instalar automáticamente si el usuario no responde a las alertas; o simplemente escoja **Do not set a deadline for software update installation** si quiere que las actualizaciones estén siempre para elegir e instalar. Oprima **Next**, vea el resumen y pulse **Finish**.



La posibilidad de instalación de parches mediante SCCM es muy importante, tanto o más que la de repartir software. Su relevancia radica en poder probar las actualizaciones para que no interfieran en la continuidad del negocio. En una empresa, tenemos aplicaciones nuevas y viejas; muchas de las viejas, en ciertas ocasiones, sin soporte. Si reemplazáramos una DLL con una actualización que no contempla el uso que esta aplicación le da, puede ocurrir que la aplicación falle. Entonces, necesitaremos tener un plan de recupero, de restauración. Durante esos minutos u horas que puede llevarnos recuperar un equipo en estas circunstancias, la empresa pierde dinero. Puede perder dinero por la aplicación que tiene el servidor, pero también pierde accionar y respuesta de su equipo de IT por estar atendiendo un problema que no debería haberse originado. Por eso, es muy importante probar los parches, tener varios niveles de implementación y, así, lograr un mayor control de los posibles cambios en los sistemas más delicados.

Análisis y seguimiento de parches

El análisis y el seguimiento de los parches es muy sencillo, parecido al de los paquetes de software. Podemos ver los detalles de los paquetes de distribución en: **Site Database/Computer Management/Software Updates/Deployment Packages**.
Los paquetes se irán instalando, y en esta ubicación podemos ver los detalles de los puntos de distribución, si se instalaron en ellos o no, un listado de las actualizaciones y algunos permisos a nivel accesos de seguridad. Lo más importante en el seguimiento son los reportes. En la página de Reportes (que después veremos dónde se ubica y sus detalles) tenemos miles de reportes para sacar de SCCM. Por ahora, veremos los reportes desde la consola principal. Si vamos a **Site Database/Computer Management/Reporting/Reports**, tendremos un listado de reportes. Allí buscamos uno llamado: **Compliance 1 – Overall Compliance**. Hacemos clic derecho sobre el reporte y elegimos **Run**. Se nos pedirá un Update List y una colección.
Tengamos en cuenta que los reportes se sacan desde la base de datos. Esto no es una consulta en el momento a los clientes, sino una consulta a los datos que informan los clientes. Por ende, pasarán unas horas hasta que comencemos a ver los avances. Con este informe tenemos una leve vista de cómo van avanzando nuestros parches



AUDITORÍAS

Cada paquete armado en SCCM tiene un número que lo distingue. Los auditores de entornos IT necesitan distinguir los cambios realizados en los sistemas, y este número es de gran ayuda para lograrlo. Debemos demostrar que tenemos nuestro entorno de prueba de parches y aprobación de parches con sus pedidos de cambio para satisfacer los requerimientos.

en la empresa. Luego, tenemos más informes que podemos ir analizando, pero éste es el que engloba todos los resultados. El mismo informe puede ir sacándose para las distintas colecciones de nuestros templates y, así, ir viendo el avance de la instalación.

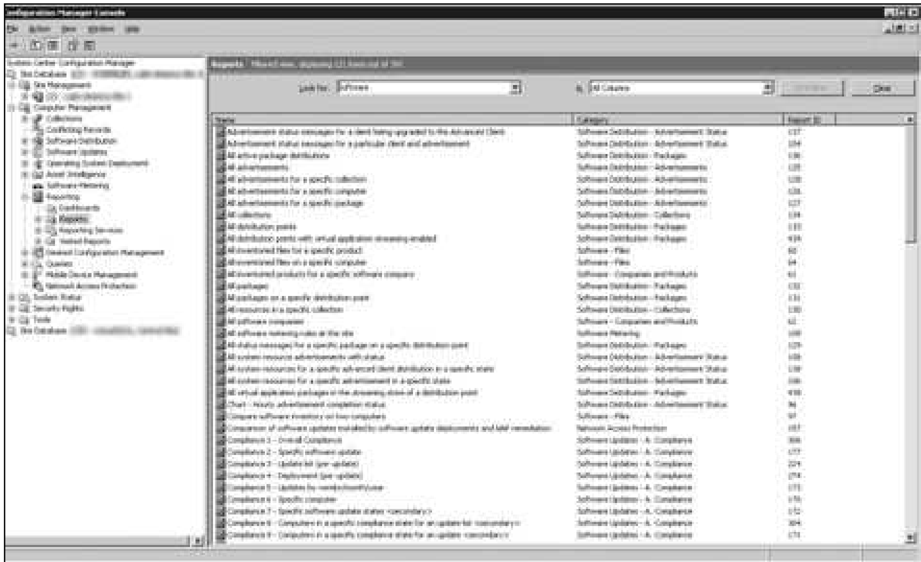


Figura 5. *En la figura se ven las propiedades del rol Reporting Point, instalado por default en el servidor principal. Aquí se define el sitio web en el que se revisarán los reportes.*

REPORTES

Llegamos por fin a la característica de SCCM que lo hace realmente único entre las soluciones del mercado. La gran lista de reportes de información que podemos obtener de nuestra infraestructura es increíble. SCCM se encarga de convertir millones de datos que tenemos dando vueltas por la empresa, y transformarlos en información, lo cual les da un valor agregado incalculable. Existen dos tipos de reportes principales que analizaremos: los reportes en línea contra la base de datos y los reportes programados utilizando Reporting Services de MsSQL.

Qué son los reportes en SCCM

Los reportes representan el mayor valor agregado de todo SCCM; es por lo que realmente vale la pena tenerlo. Los reportes son millones de datos convertidos en información. Éste es el fin de todo sistema de información, pero SCCM lo hace muy bien. Millones de datos andan rondando las fronteras de la empresa sin que

nadie les dé mucha importancia. Si nos ponemos a analizar, hay muchas cosas que saber. Pongamos un ejemplo. Los dirigentes quieren empezar a utilizar OCS, la famosa herramienta de comunicación interactiva de Microsoft. Ésta emplea el framework de .NET 3.5. Este paquete de software ocupa unos 300 MB. Supongamos que lo quieren implementar cuanto antes, pero hay mucha variedad de máquinas y varias con poco espacio en disco. Para saber si la idea es viable, podemos sacar un reporte de espacio en disco para todas las máquinas de la empresa. Así, sabríamos cuánto es necesario gastar en renovación de discos o de máquinas para efectuar la implementación de OCS. También puede suceder que queramos comenzar a utilizar un software que consuma mucha memoria; en ese caso, podemos sacar un informe de cantidad de memoria en las máquinas, para conocer el costo real de la implementación que realizaremos.

Debemos tener en cuenta que sin esta tecnología, deberíamos ir haciendo un cuestionario máquina por máquina, si no las tenemos relevadas de antemano. Sería muy complicado saber los costos reales de la implementación de un nuevo software sin SCCM. Es importante tener presente que este sistema nos permite obtener reportes de cualquier situación que se nos ocurra relacionada con inventario de hardware, de software y uso de los equipos. SCCM consume la información enviada por sus clientes y la almacena en una base de datos. El rol específico que realiza esta tarea es el Management Point. El servidor que tenga este rol estará a cargo de enviar la información a la base de datos. Esta base tiene mucha información, y es de allí de donde nacen los reportes. Cuando queremos sacar un reporte, se efectúa una consulta a esta base de datos. Al contrario de lo que uno supondría, no se crean consultas a los clientes cada vez que queremos hacer un reporte. Por lo tanto, siempre hay un tiempo de diferencia entre que el cliente informa los cambios de su inventario, de sus actualizaciones, etcétera, hasta que SCCM pueda informarlo. Es muy importante tener esto en cuenta, porque varios gerentes comenzarán a preguntarnos por los resultados en cuanto comencemos a realizar esta tarea. Debemos estar atentos y explicar el porqué de estos tiempos.

Anteriormente, aprendimos cómo ver los reportes desde la consola, pero SCCM también nos da la posibilidad de ver los reportes desde un sitio web que publica el Management Point. El servidor necesita tener el rol de Reporting Point instalado.



PERMISOS A LOS REPORTES

Es muy importante que nos demos a la tarea de administrar bien el acceso a los reportes. Para poder verlos, es necesario cargar el usuario en un grupo llamado **SMS Reporting Users** en el equipo que tiene el rol instalado y, posteriormente, agregarlo en **Site Database/Security Rights/Users** con los permisos de lectura correspondientes.

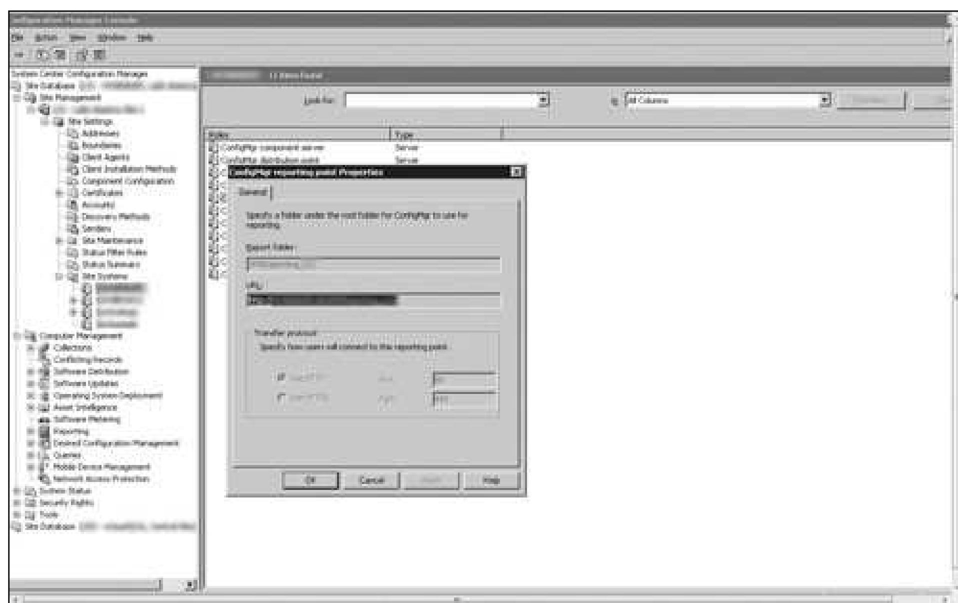


***Figura 6.** En la figura se ven las propiedades del rol Reporting Point instalado por default en el servidor principal. Aquí se define el sitio web en el que se revisarán los reportes.*

El sitio web nos mostrará un árbol a la izquierda con todos los reportes que podemos sacar desde SCCM: los que trae predefinidos y los que nosotros creemos. A la derecha, nos mostrará las opciones de cada uno. En muchos de ellos, las opciones básicas son agregar una colección específica y algún que otro dato.

El reporte que se muestre al pedir los resultados puede imprimirse, exportarse como archivo CSV, mandarse por mail o copiarse. Luego, tenemos otra forma de ver reportes, que es a través de Reporting Services. Este servicio es una característica de MsSQL, pero se integra a SCCM instalando un rol específico que veremos más adelante. Esto nos instala otro sitio web que nos dará un menú mucho más amigable e interactivo. Este sitio web tendrá la particularidad de que podremos dar permisos de acceso a los reportes y, también, suscribirnos a ellos para recibirlos cada determinado tiempo que designemos. Concluyendo, los reportes son datos



IMPORTANCIA DE LOS REPORTES

La posibilidad de tener estas clases de reportes con SCCM significa demostrar el avance en ciertos trabajos que antes no había manera de evidenciar. Usarlos y exponerlos a las altas gerencias nos dará una cuota de credibilidad en todo el accionar diario, y es una forma humana de demostrar los resultados a personas que no entienden de IT.

combinados que generan información valiosa al analizar un problema específico. A continuación, veremos algunos reportes bastante importantes que nos servirán en la administración diaria de nuestra infraestructura.

Reportes importantes

Hay miles de reportes, y tomarnos un tiempo para analizar los que realmente aportan valiosa información a las tareas diarias y a los gerentes de la empresa nos resultará muy útil en nuestra carrera como profesionales. Hay muchos en SCCM, y nosotros mismos podremos crear varios más, pero aquí sólo mostraremos algunos. Para ingresar a la página de reportes, necesitamos ir a la dirección: **http://Nombre_del_servidor_SCCM/SMSReporting_nombre_del_site/Reports.asp**.
Una vez que ingresamos al sitio, veremos una página similar a la de la **Figura 7**. Luego, debemos elegir el reporte que queremos.

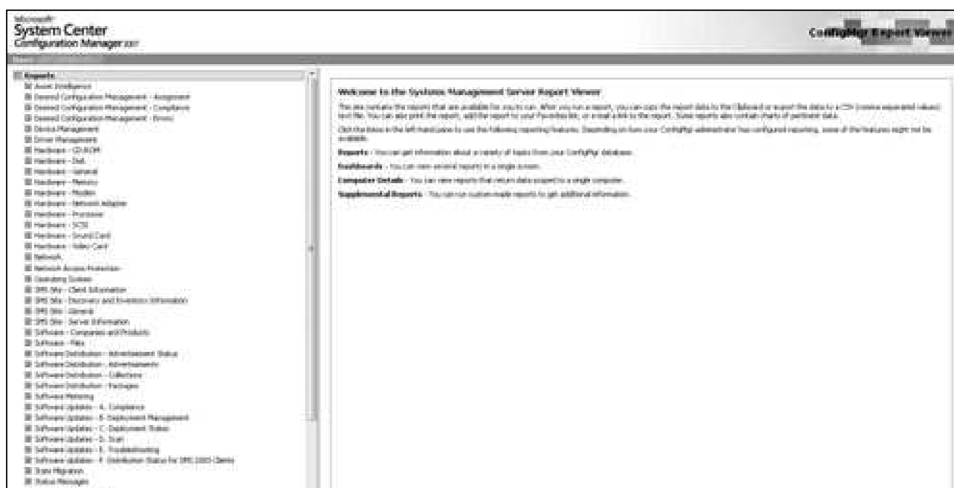


***Figura 7.** Veremos el árbol de reportes de SCCM en el lado izquierdo, y las opciones en el derecho. Al elegir un reporte y llenar los campos requeridos, éste se mostrará en una ventana emergente.*

El primer reporte que vamos a analizar es el de inventario. Para ingresar en cada reporte debemos ir expandiendo cada opción del árbol mientras oprimimos la tecla **+**. Si queremos ingresar en el de inventario, por ejemplo, vamos a: **Reports/Asset Intelligence/Hardware 01A- Summary of computers in specific collection**.
En muchos casos, puede ser que la base de datos tenga demasiados valores y no muestre todo el listado real de los posibles datos por elegir. Por ejemplo, cuando tengamos que indicar el nombre de un software, debemos buscar el valor por nombre. Podemos escribir el nombre o parte de él, y usar como comodín el signo **%**. Este signo puede colocarse tanto adelante, atrás o en el medio, para realizar distintas

combinaciones. Si indicamos, por ejemplo, **All Systems** en el campo de colecciones y oprimimos el botón **Display**, se abrirá otra ventana del navegador con los resultados.

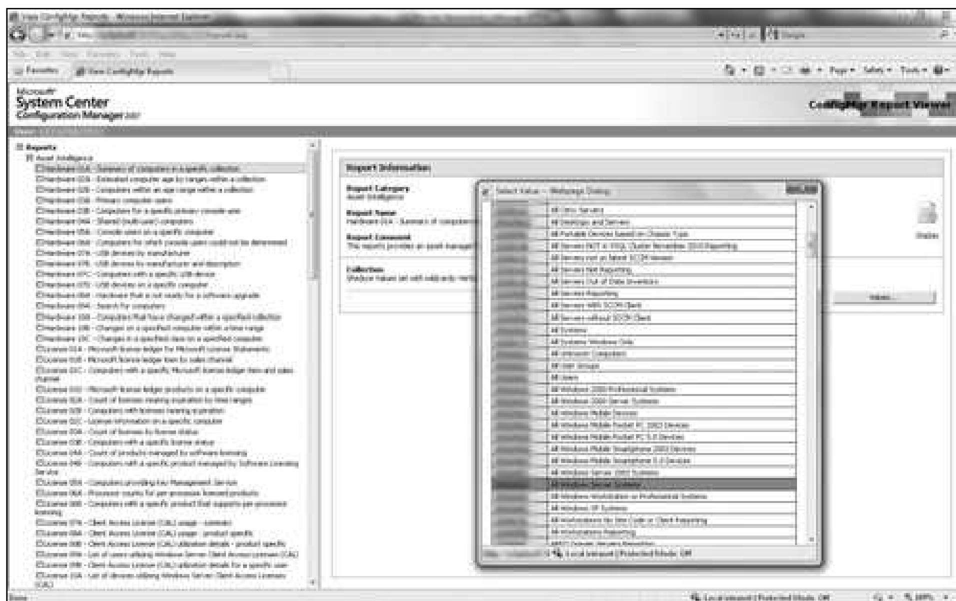


***Figura 8.** Si oprimimos Values..., se abrirá una ventana emergente con un listado de las posibles colecciones que podemos elegir.*

Casi todos los resultados se muestran de la misma manera: un título con detalle en la parte superior y, debajo, una tabla con los detalles. En este caso, se indicarán varios datos importantes:

- Nombre de equipo
- Dominio
- SMS Site
- Usuario de consola top
- Sistema operativo
- Nivel de Service Pack



ANÁLISIS DE SOFTWARE EN LA EMPRESA

Debemos saber que podríamos trabajar con el departamento de seguridad para analizar el software permitido en la empresa. Pueden surgir desagradables sorpresas al analizar las máquinas que contienen algún software indeseable para la organización. Algunas veces se descubren grandes robos de información y agujeros de seguridad importantes.

• Número de serie
• Empresa manufacturera
• Modelo
• Memoria RAM
• Procesador (GHz)
• Tamaño del disco rígido
• Espacio libre en disco rígido

Algunos campos que siempre figuran son fecha y número de filas y, arriba de todo, habrá unos botones para copiar, exportar, imprimir, agregar a favoritos y, también, una opción de e-mail. La opción de favoritos es porque podemos volver a ingresar en este reporte con estas opciones cuantas veces queramos; obviamente, siempre con los mismos parámetros que indicamos antes. Sólo oprimiendo en el link, se mostrará el informe. Al costado izquierdo, la mayoría de los reportes tienen un acceso directo. Hay algunos que no lo poseen, pero en los que está presente, tenemos la posibilidad de acceder a un detalle de esa fila.
Otro reporte importante es el de análisis de software instalado que figura en **Agregar o quitar programas**. Debemos tener en cuenta que el reporte nos entregará un completo listado de todas las máquinas que tengan determinado software registrado en el sistema operativo. Para ingresar al reporte correspondiente debemos utilizar la dirección: **Reports/Software – Companies and Products/Computers with specific software registered in Add and Remove programs**.



***Figura 9.** Hay miles de programas en la base de datos; debemos ayudarnos con el comando % para buscar uno en particular. Abajo, otra vez elegimos una colección.*

Este reporte nos brindará un reporte básico, en el que sólo figurarán como datos importantes: nombre del equipo, dominio, usuario y sistema operativo. A diferencia del anterior, no sólo necesita que elijamos una colección correspondiente, sino que también debemos seleccionar un software.

El próximo reporte es un poco extraño y suele fallar si el SCCM no está actualizado con el último parche disponible. Este reporte informa la edad de los equipos, nos indica por año la cantidad de máquinas que tenemos en la empresa. Este reporte a veces falla, más que nada, con los equipos nuevos. El análisis es muy simple. El reporte se construye a partir de los datos del BIOS. Como está creado contra un listado en alguna tabla de SCCM, puede ser que, en la tabla, al momento de crearse por parte de Microsoft, los nuevos BIOS no estén cargados. Entonces, el reporte no nos indica ninguna información. Accedemos a él desde: **Reports/Asset Intelligence/ Hardware 02A – Estimated computer age by ranges within a collection**.

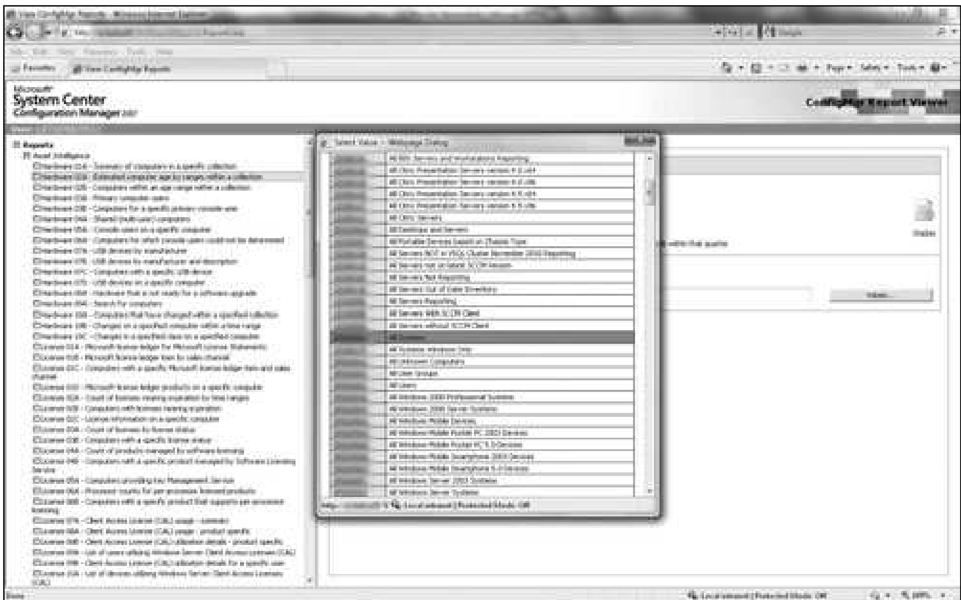


***Figura 10.** También este reporte necesita una colección; con tan sólo ese dato, nos dará los resultados de todos los equipos en ella.*



BIOS

Proviene de la sigla **Basic Input-Output System**, y es un firmware que viene en todos los equipos; es el primer programa que se ejecuta al encender el sistema. Las empresas que producen placas madre tercerizan la creación de los BIOS a los principales fabricantes, que son American Megatrends, Phoenix Technologies, General Software, Insyde Software, y otros.

El resultado de este reporte será una cantidad de filas que describen lo sucedido en cada trimestre del año. Entonces, por ejemplo, si una máquina fue construida en el segundo trimestre del año 2005, figurará en la fila que se distingue como **2005/Q2**. Los equipos que queden fuera de este informe por ser nuevos estarán sumados en la fila denominada **(Not Available)**. Estas filas se muestran en la **Figura 11**.

Figura 11. *Las máquinas que queden fuera de este informe por ser nuevas estarán sumadas en la fila llamada* ***(Not Available).***

A continuación, veremos dos informes importantes a nivel sistema. Uno es un reporte que nos indica las máquinas con determinado sistema operativo, en tanto que el otro es para ver las fallas de las instalaciones de los clientes de SCCM. Al primero se accede desde la ruta: **Reports/Operating System/Computers with a specific operating System**.

Figura 12. *En este reporte indicamos el sistema operativo Windows que queremos analizar. Es muy útil para calcular el total de sistemas de cada versión en la empresa.*

Junto a este reporte de sistemas operativos nos serán útiles otros, como **Count Operating System versions** y un grupo de reportes de licencias ubicados en **Asset Intelligence**. Con ellos podremos obtener la cantidad de licencias utilizadas para cierto producto, las licencias a punto de caducar y varios datos más que nos darán un pantallazo acerca de lo que está sucediendo en nuestra empresa con las licencias.
Para acceder al reporte de fallas de instalación del cliente SCCM, debemos ingresar a: **Reports/SMS Site- Client Information/Client Deployment Failure Report**.
Este reporte no necesita ningún dato; sólo oprimimos en **Display** y nos traerá un listado de máquinas y la posible falla por la que no se pudo instalar dicho cliente.

***Figura 13.** Vemos en el reporte el nombre del equipo, la fecha del intento de instalación y la descripción de la posible falla.*

Los últimos dos reportes que veremos son para el seguimiento de la instalación de parches y de software. Uno es para acceder al listado de parches en una implementación de un paquete de actualizaciones. Nos indica un listado de todas ellas accediendo a la



SOFTWARE LEGAL

Firmas como Adobe, Microsoft, Symantec, y otras tienen grupos sin fines de lucro dedicados a vigilar a las empresas y las licencias de productos. Según la legislación de cada país, se incluyen multas a aquellas organizaciones que no cumplan con los pagos correspondientes. A nivel internacional, las agencias se agrupan en la Business Software Alliance: **www.bsa.org.**

ubicación que se encuentra en **Reports/Software Updates-B. Deployment Management/ Management 2 –Updates in a deployment**.

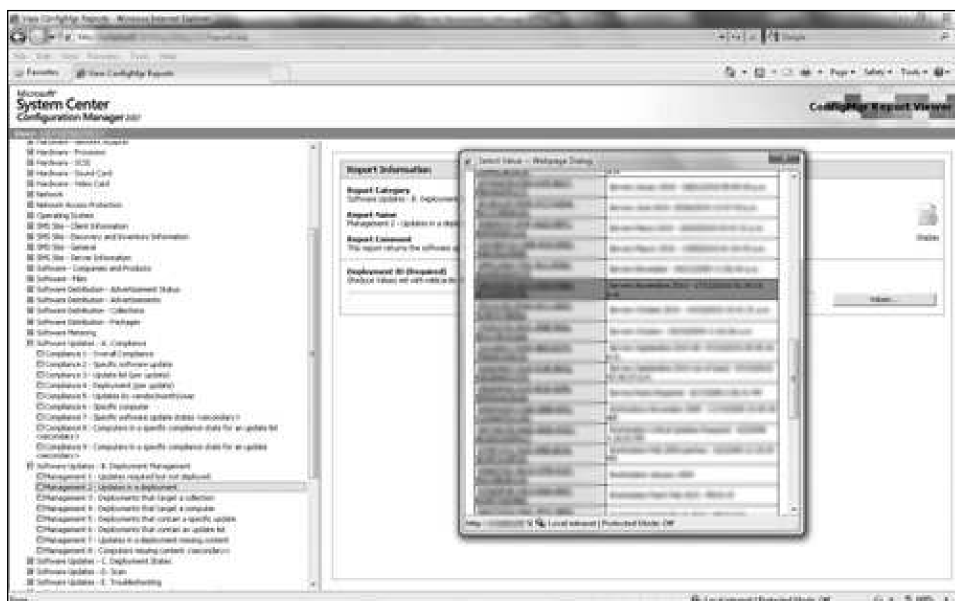


***Figura 14.** En este reporte figurará la clave única en la base que distingue a ese paquete de actualizaciones implementado, muy importante para los sistemas de auditoría.*

El último de este análisis es un reporte que nos indica el estado de una advertencia de software. Con este reporte podemos ir viendo el avance de la instalación de un paquete en toda la empresa o en las máquinas a las cuales fueron asignadas: **Reports/Software Distribution-Advertisement Status/Status of a a specific advertisement**.



***Figura 15.** En este reporte debemos elegir una de las advertencias que hayamos lanzado; podemos buscar el nombre de la misma forma que en los reportes anteriores.*

A continuación, veremos cómo instalar Reporting Services, una muy buena característica que trae SCCM para programar reportes sobre nuestra infraestructura.

Cómo instalar Reporting Services

Explicaremos en simples pasos cómo programar reportes automáticos con SCCM 2007 SP2. Esto puede hacerse gracias a Reporting Services, que viene con MsSQL 2005. Si no tenemos esta característica instalada, debemos instalarla en el servidor. Tenemos que montar el DVD de SQL 2005 en el servidor o la versión que hayamos instalado. Luego, pasamos los prerrequisitos del ayudante de instalación. Para actualizar una base de datos de Reporting Services que ya exista, una base que hayamos tenido instalada de antemano, debemos correr el instalador del DVD con el parámetro **SKUUPGRADE=1**. Esto actualizará la base de datos en cuestión y no tratará de instalar una nueva. La instalación de Reporting Services no demanda mucho tiempo. Para realizar el proceso de instalación y también la integración con SCCM necesitamos tener SCCM R2 instalado en la computadora, SQL Reporting Services, IIS 6.0 o más actual, y también, SQL Server Business Intelligence Development Studio para acceder a modelar los reportes nuevos. En nuestro site necesitamos tener instalado SCCM 2007 R2 como mínimo y el rol de Reporting Services en el servidor principal que contenga el site.
Una vez que hayamos pasado los prerrequisitos del instalador de MsSQL, elegimos instalar Reporting Services. Luego de instalar la característica de SQL, reiniciamos el servidor y corremos el ayudante de configuración **Reporting Services Configuration**.

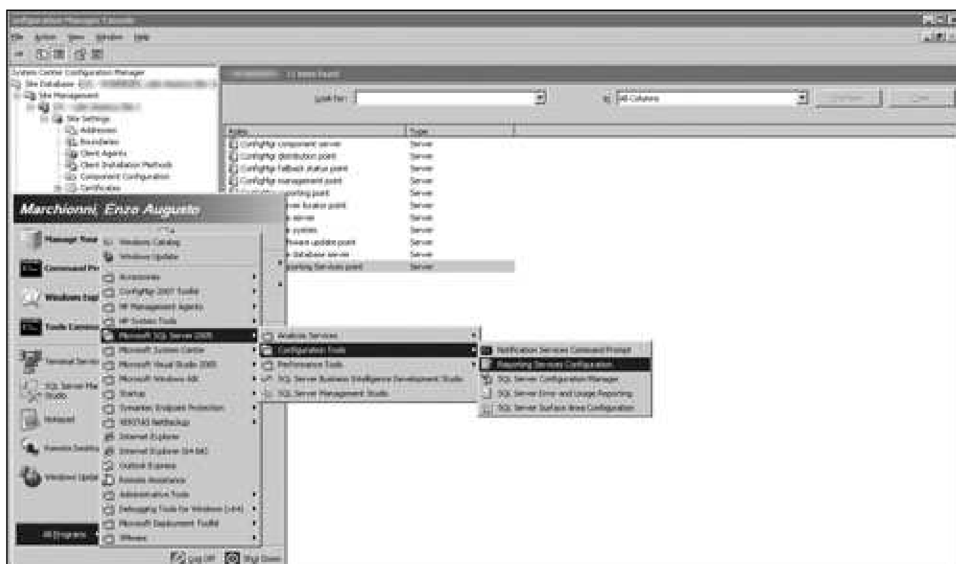
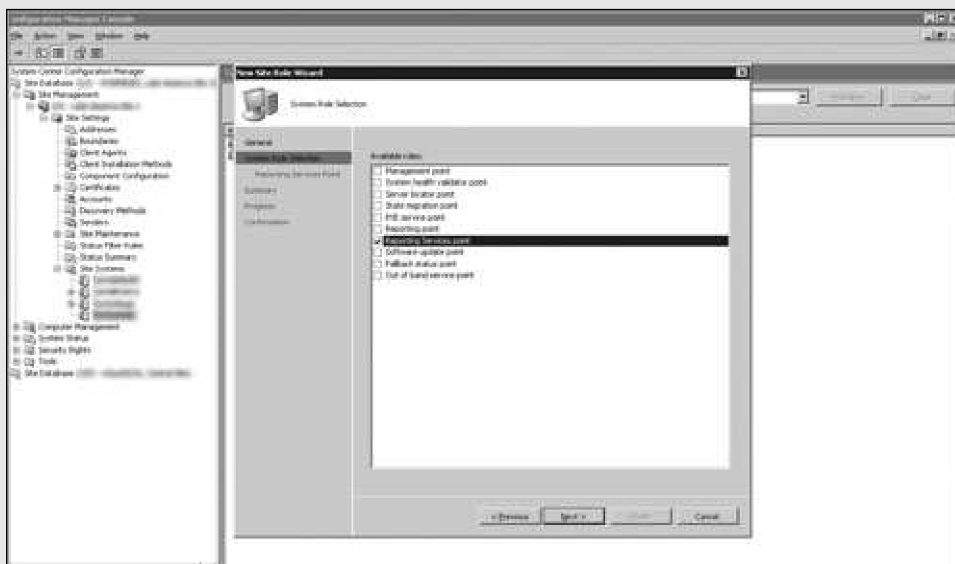


Figura 16. *El ayudante de configuración de Reporting Services se encuentra en el menú de inicio una vez instalado.*

Algo que puede ocurrir es que, al querer ejecutar la configuración, nos dé un error sin solución aparente ni en Internet ni en ningún lugar o foro de SQL. Si queremos actualizar un SQL Server con el CD anterior al SP2 cuando el SP2 ya lo tenemos instalado, obtendremos un error. Lo que sucederá en este caso es que Reporting Services se instalará con archivos de una versión vieja y dejará configuraciones anteriores al SP2. Para solucionarlo reinstalamos SQL SP2. Luego podremos ejecutar sin problemas el ayudante de Reporting Services, que creará el site para los reportes. Entonces, definimos los usuarios, creamos la base de datos y configuramos un par de temas más, como el SMTP para mandar los mails. Después de ejecutar el ayudante y de que todo haya quedado configurado, instalamos el rol en el SCCM.

Instalar el rol de Reporting Services — PASO A PASO

1 Vaya a la consola de SCCM, hasta el servidor que tenga la base de Reporting Services recién creada. Instale un nuevo rol y seleccione **Reporting Services point**.

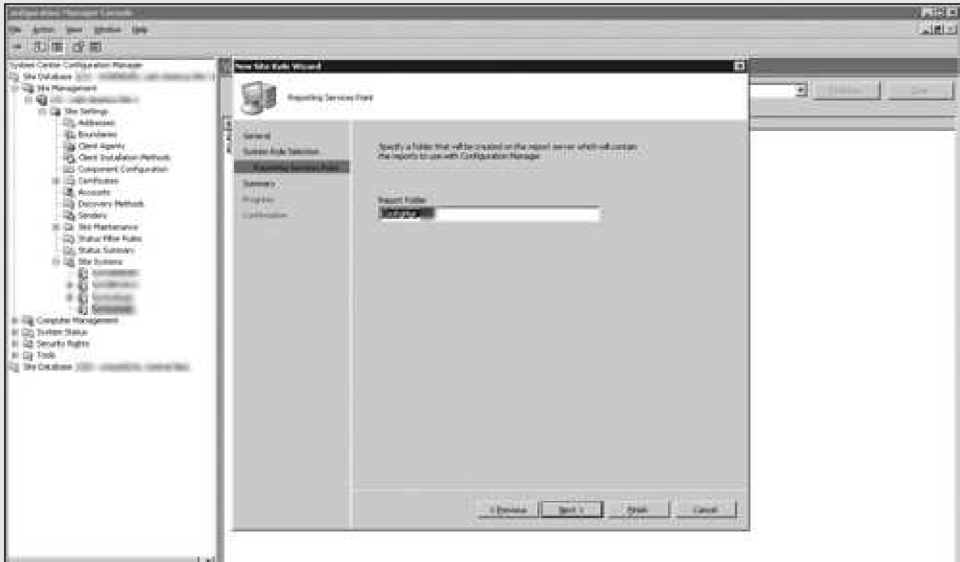


REPORTING SERVICES

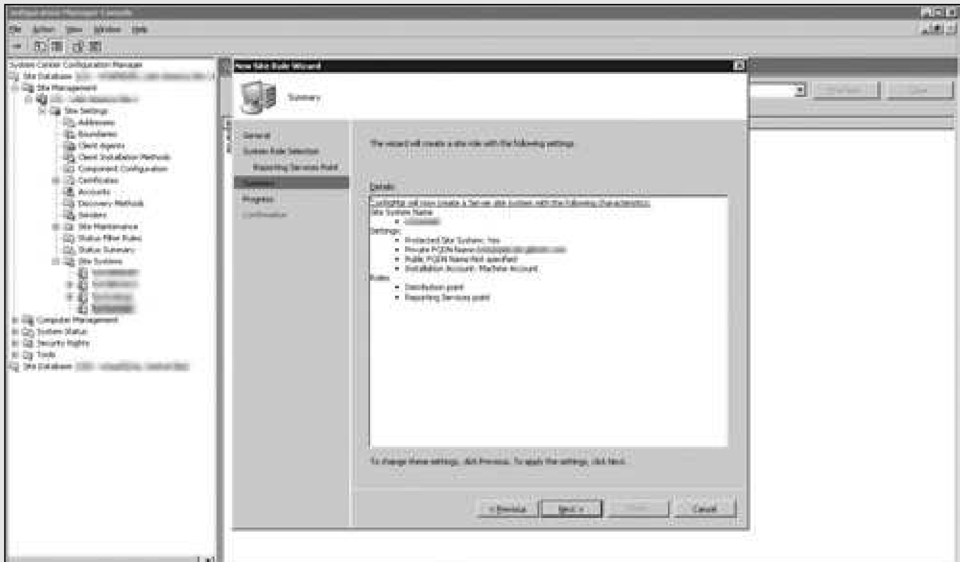
Debemos tener en cuenta que es posible encontrar información adicional sobre SCCM y también sobre Reporting Services de forma conjunta en el sitio web que se encuentra en la dirección **http://technet.microsoft.com/en-us/library/cc431393.aspx.** Aquí se expone la relación de estas dos tecnologías, prerrequisitos, planeamiento de la instalación y solución de problemas.

▶

2 Para continuar, deberá colocar el nombre correspondiente a la carpeta principal que contendrá los reportes en el sitio web. El nombre debe ser representativo.



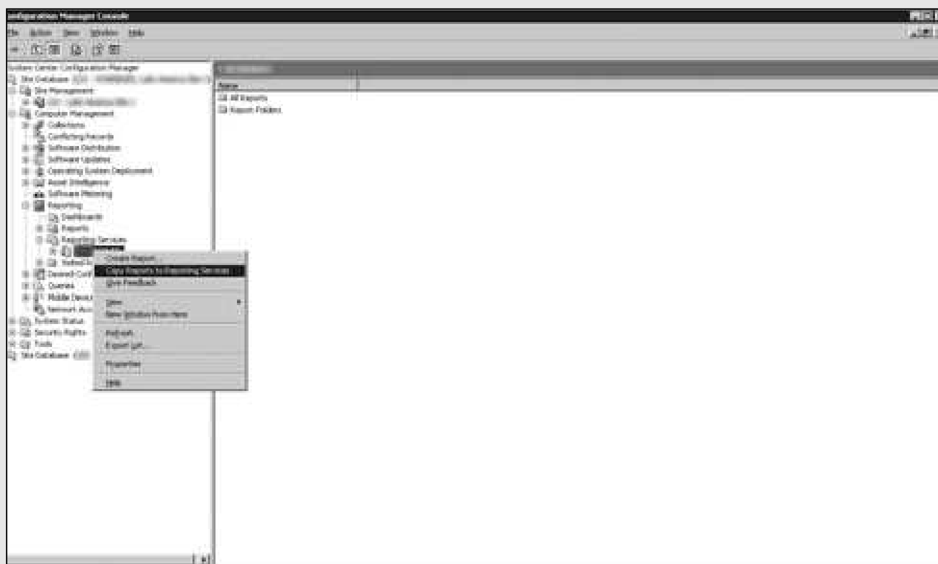
3 A continuación podrá ver el resumen correspondiente; será necesario que se asegure de que el texto corresponde a la tarea que está realizando. Para continuar, haga clic sobre el botón denominado **Next** y posteriormente presione sobre **Finish**; de esta forma terminará la instalación del rol.



▶

►

4 Diríjase a **Database/Reporting/Reporting Services** y seleccione el servidor de reportes. Haga clic derecho y elija **Copy Reports to Reporting Services**.



En el último paso, copiamos los reportes ya creados de SCCM a la carpeta de Reporting Services. Todos los reportes a los que antes accedíamos desde el sitio **http://Nombre_del_servidor_SCCM/SMSReporting_nombre_del_site/Reports.asp** podrán ser accedidos desde el nuevo sitio de Reporting, que tendrá una dirección similar a: **http://Nombre_del_servidor_SCCM/Reports/Pages/Folder.aspx**. Entonces, podremos disfrutar de todos nuestros reportes de forma más interactiva, ya que accederemos a cada uno de ellos y seleccionaremos las opciones de una lista desplegable sin ventanas emergentes. La característica principal es que podremos programarlos para que sean enviados cada determinado tiempo. A continuación, aprenderemos a programar un reporte para que llegue automáticamente vía e-mail.

Automatizar reportes

La automatización de reportes, como ya mencionamos, es la característica más importante de SCCM. Con ella podremos seguir de cerca instalaciones de parches y de hardware, errores y todo tipo de información, recibiendo todo directamente en nuestra casilla de correo. Estos reportes pueden programarse de forma diaria o cada hora. Existe una enorme flexibilidad de programaciones de días y horario. Para determinados reportes, podremos tener distintas programaciones, cada una denominada suscripción. Entonces, podríamos programar un seguimiento de instalación

de parches diario y un resumen mensual. Estas programaciones pueden tener distintos destinatarios, y no es estrictamente necesario que sean los mismos. Puede haber varias suscripciones para un mismo reporte.

Las suscripciones nos permitirán mandar informes a nuestros gerentes de manera periódica, sin ninguna intervención más que su programación, única y sencilla. Nuestro correcto proceder una vez que tengamos esta capacidad es hacer un análisis de los reportes que pueden llegar a interesar a nuestros jefes o a nosotros, presentarlos y acordar un período conveniente. A continuación, veremos un ejemplo práctico en el que configuraremos un reporte para que sea enviado por e-mail.

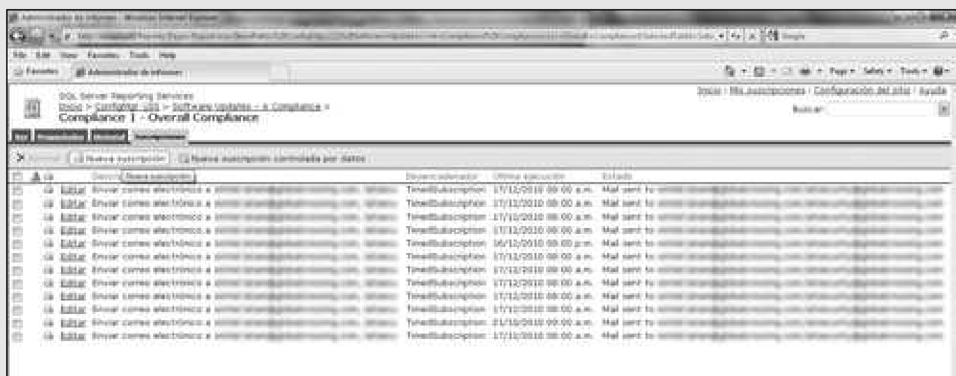
Programar un reporte con Reporting Services

PASO A PASO

1 Vaya hasta el sitio de Reporting Services de su site de SCCM. Expanda las carpetas y elija un reporte por programar.



2 Haga las pruebas de los resultados y luego vaya hasta la solapa **Suscripciones**. Allí haga clic en **Nueva suscripción**.



▶

3 En la opción **Entregado por:** elija **Correo electrónico**; llene los campos adecuados y modifique el **Asunto** si lo desea. Complete las opciones del reporte en **Valores de parámetro de informe**. Luego, oprima en el botón **Seleccionar programación**.

4 Elija las opciones de **Programación diaria** que más le convengan; debe seleccionar los días y las repeticiones. Indique un horario y seleccione **Fechas de inicio y fin**.

Con estos simples pasos, podrá configurar reportes para el área de helpdesk, ejecutiva, administración, auditoría, etc. La información creada por SCCM genera valor agregado dependiendo de las personas a las que esté dirigida.

BASE DE DATOS DE SCCM

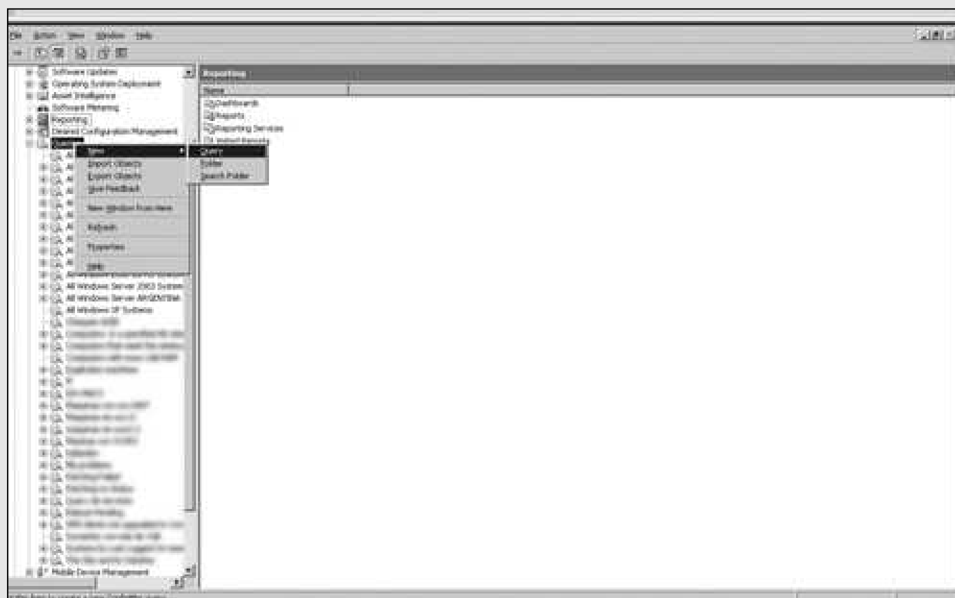
SCCM no podría funcionar si no fuese por su base de datos. Éste es su corazón, el centro de información que sirve a toda la compañía. Desde allí se obtienen los datos que se analizarán luego mediante los reportes. Es muy importante tener una buena administración y mantenimiento para que no haya problemas de ningún tipo. No podremos analizar todas las tablas que contiene la base de datos debido a la gran cantidad; en cambio, veremos algunas tablas importantes y aprenderemos a realizar consultas para obtener información bajo nuestras propias exigencias y requerimientos, más allá de las consultas preestablecidas.

Consultas de SQL desde la consola SCCM

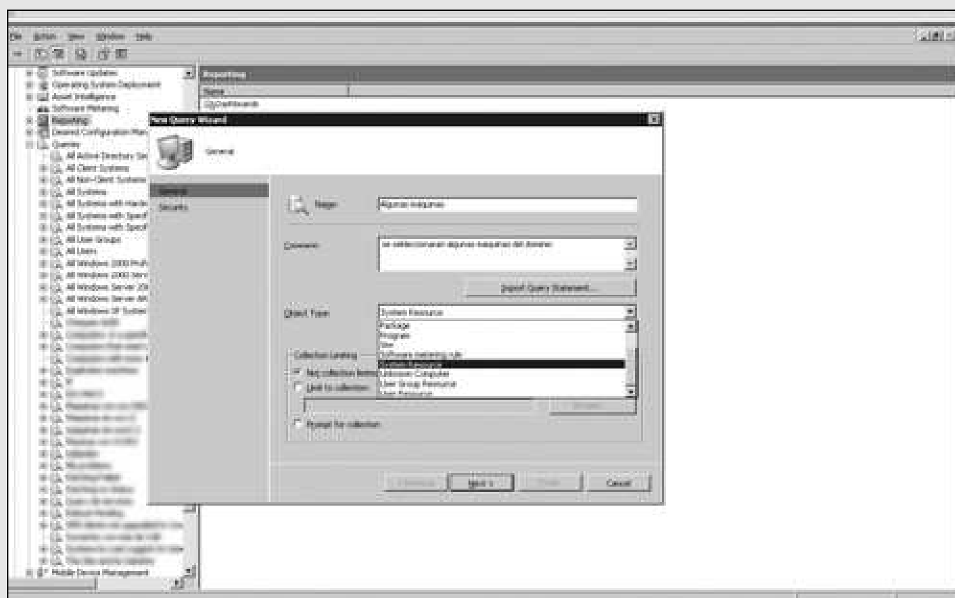
Para los administradores es muy importante tener en cuenta la posibilidad de administración de la base de datos que nos ofrece SCCM. Es interesante saber que será posible crear consultas desde la consola con las herramientas disponibles y ayudantes o, directamente, desde las herramientas correspondientes a MsSQL. Todas las colecciones y reportes están creados mediante una consulta Transact SQL. Si observamos las propiedades de cada uno, veremos la consulta SQL en ese lenguaje, que le da vida al reporte o colección. Esta consulta puede copiarse y modificarse a gusto para obtener otros resultados.
Debemos saber que uno de los usos posibles puede ser obtener una colección similar a una ya creada, pero preocupándonos de definir un criterio distinto. Desde la consola tendremos varios ayudantes destinados a generar las consultas. Éstos se ejecutarán al querer crear una colección o un reporte nuevo. Los ayudantes nos acompañarán durante todo el proceso.
Si queremos administrar consultas de SQL específicamente, SCCM nos ofrece varias herramientas desde su consola principal. Para realizar esta tarea podemos ir a **Site Database/Computer Management/Queries**, donde se mostrará un extenso listado de consultas SQL que ya han sido creadas. A continuación, revisaremos en detalle un ejemplo práctico en el que necesitamos realizar la creación de una nueva consulta que nos traiga el nombre del AD Site a la cual corresponde la máquina, el nombre y también la dirección IP de los equipos que tengan 1 GB o más de memoria RAM. Recordemos que 1 GB = 1024 MB = 1024 x 1024 KB. El caso práctico que mencionamos se comenta en detalle a continuación.

■ Crear una consulta SQL desde la consola de SCCM PASO A PASO

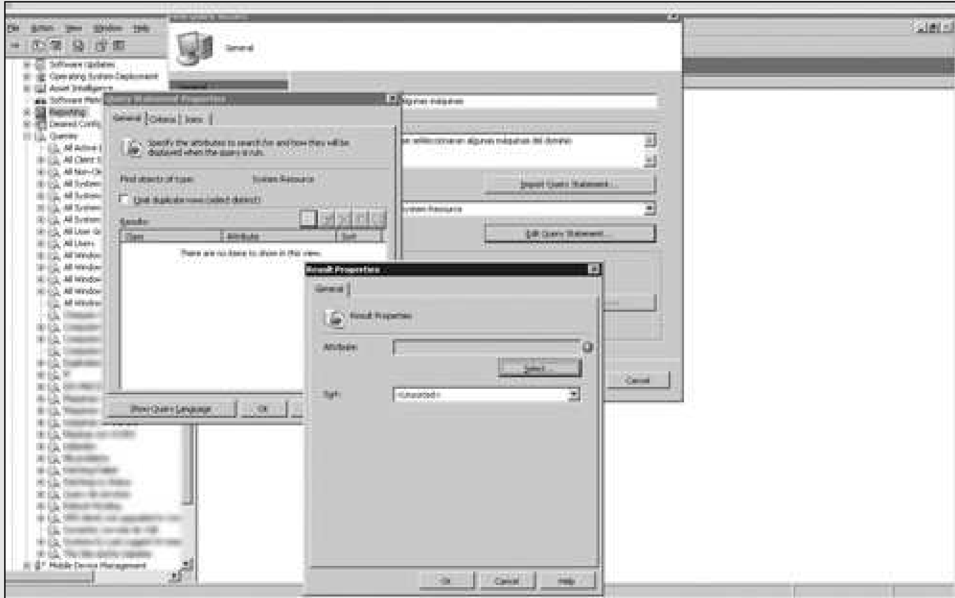
1 Diríjase a la ubicación de las **Queries**. Haga clic derecho y seleccione **New/Query**.



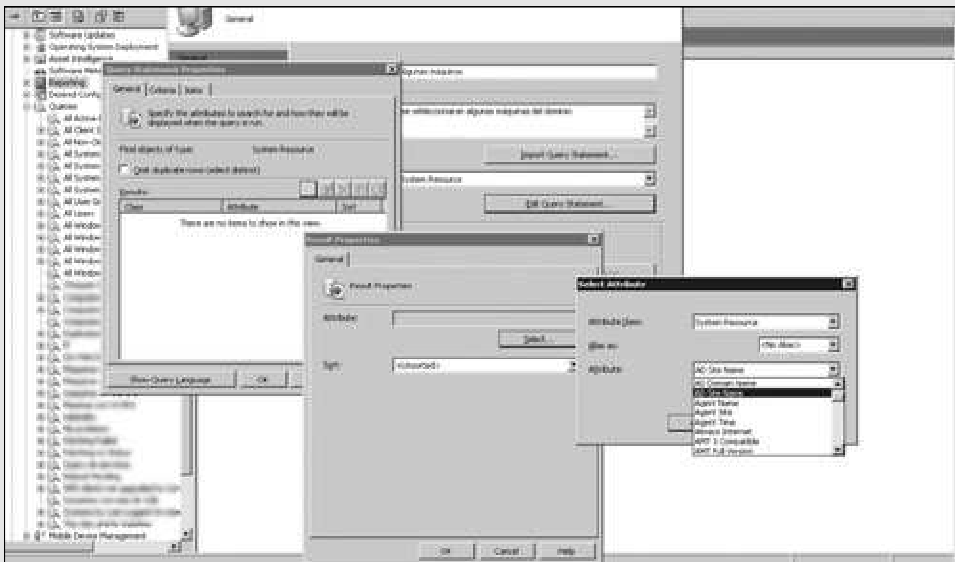
2 Escriba un nombre en **Name**, la descripción en **Comment** y elija un tipo de objeto. Oprima **Edit Query Statement**, verá este botón cuando cierre la lista desplegable.



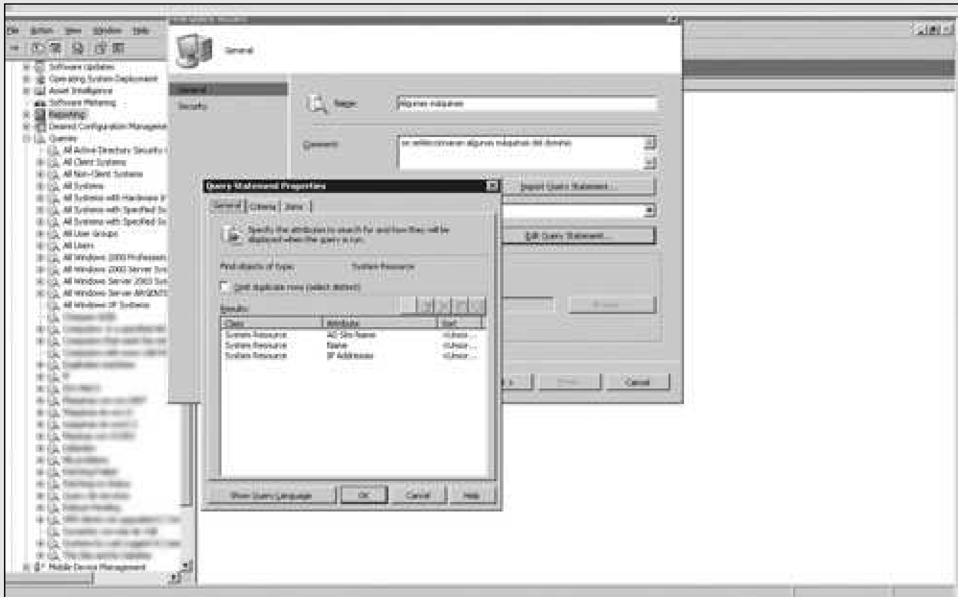
3 Se abrirá otra ventana emergente en la cual debe armar la consulta propiamente dicha. En la solapa **General** seleccione los atributos (columnas) que quiere que tenga la consulta y agréguelos oprimiendo en el botón con una estrella amarilla.



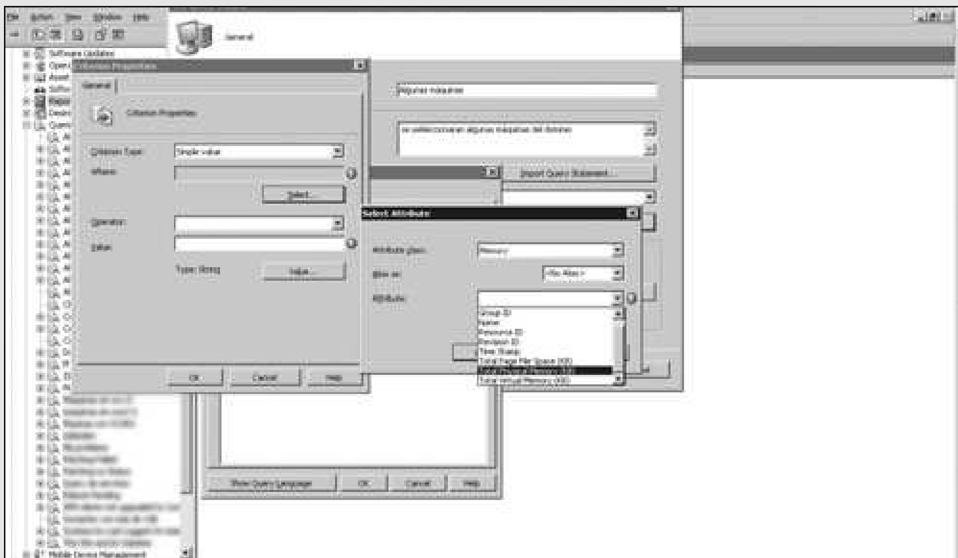
4 Presione la opción denominada **Select**, y elija la clase de atributo que desea en **Attribute class** y el nombre del atributo en **Attribute**.



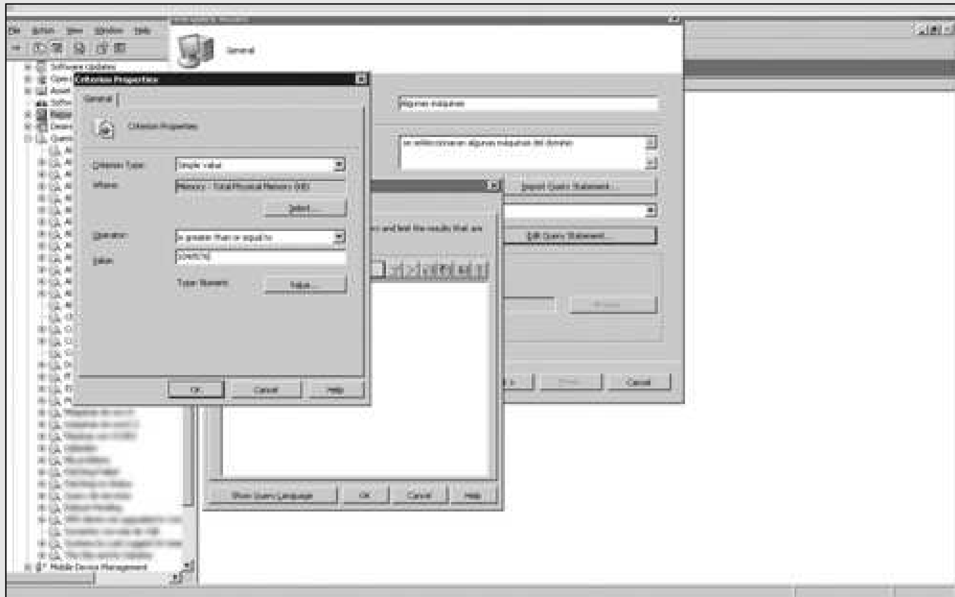
5 Una vez que haya elegido varios atributos (en este caso, tres), vaya a la solapa **Criteria** para escoger los criterios de filtro de la información requerida.



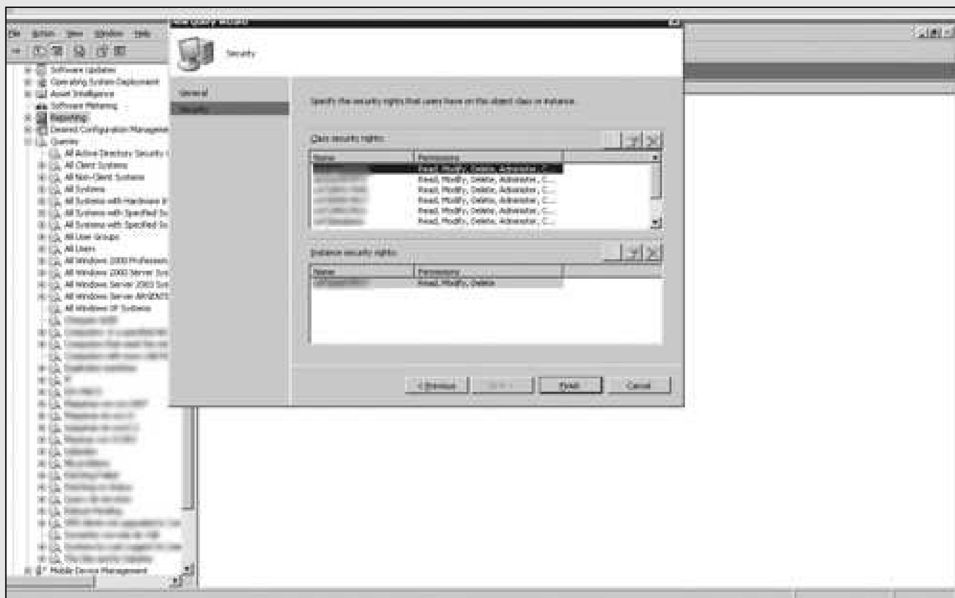
6 Oprima otra vez en la estrella amarilla para agregar criterios de búsqueda. Seleccione el tipo de criterio en **Criterion Type** y pulse **Select** para colocar el valor lógico de un atributo; elija una de las varias opciones que hay.



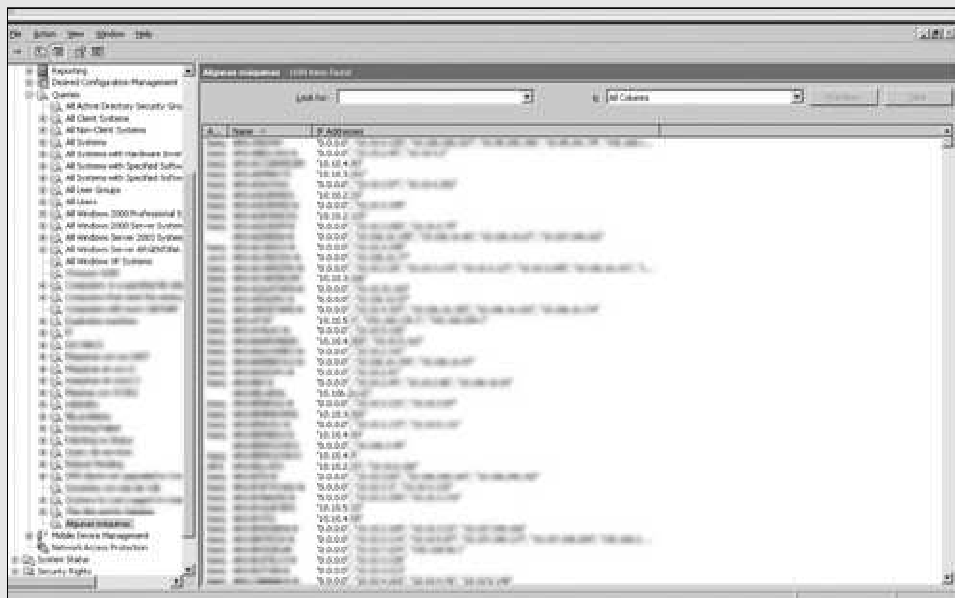
7 Seleccione el atributo **Memory - Total Physical Memory (KB)** con el argumento lógico **is greater than or equal to** y complete la opción de **Value** con **1048576**.



8 Oprima el botón denominado **OK** en todas las ventanas abiertas, pulse sobre **Next**, vea el resumen de seguridad y presione **Finish**.



▶
9 Por último, para comprobar los resultados diríjase a la sección llamada **Queries** y busque la consulta por el nombre ingresado anteriormente. De inmediato podrá ver los resultados al costado derecho de la pantalla.



Desde el apartado **Queries**, podremos observar la definición de varias colecciones ya creadas con la instalación de SCCM. Como antes dijimos, este conocimiento nos ayudará a desarrollar consultas más avanzadas y crear nuestras propias colecciones con los requerimientos que se nos ocurran.

Consultas avanzadas a la base de datos

Para crear consultas más avanzadas, podemos utilizar las herramientas de MsSQl directamente. Cuando importemos una consulta desde la definición de una colección o



TRABAJOS EN SCCM

Hace unos años, las empresas utilizaban WSUS para administrar sus parches, una herramienta simple. Hoy, en el año 2011, SCCM trae muchísimas más opciones y configuraciones. Muchas empresas grandes están comenzando a buscar administradores exclusivos de SCCM para sus equipos de IT. Estos trabajos requieren de conocimientos avanzados y son bien remunerados.

desde la definición de un reporte, es preciso tener cuidado porque, al querer ejecutar esa consulta tal como está en el analizador de consultas de MsSQL, nos dará un error. Por ejemplo, si vemos la definición de la colección **All System**, observaremos las siguientes líneas en las propiedades de la colección, más precisamente, en **Membership Rules**:

```
select
SMS_R_SYSTEM.ResourceID,
SMS_R_SYSTEM.ResourceType,
SMS_R_SYSTEM.Name,
SMS_R_SYSTEM.SMSUniqueIdentifier,
SMS_R_SYSTEM.ResourceDomainORWorkgroup,
SMS_R_SYSTEM.Client
from SMS_R_System
where SMS_R_System.ADSiteName = “ARG” or SMS_R_System.ADSiteName = “LAARG”
```

Si importamos estas líneas así como están a la consola de MsSQL, nos dará un error. Si revisamos las tablas de la base de datos, no encontraremos la tabla **SMS_R_System**, sino que su nombre es muy similar. Extrañamente, SCCM utiliza otro nombre de manera interna para llamar a las tablas en sus consultas.
Si tenemos algo de conocimientos sobre SQL, sabemos que las bases de datos también trabajan con **vistas**. Éstas son **consultas predefinidas** programadas en la base de datos, que se actualizan cada vez que se las utiliza. Esto es mucho más rápido que crear una consulta nueva, porque es manejada con el motor de la base de datos de una forma mucho más ágil y rápida que cualquier lenguaje de programación estándar. Entonces, si buscamos en las vistas, veremos una en que la tabla buscada se denomina **v_R_System**. Es como si necesitáramos reemplazar SMS por v. Si nos fijamos en otras tablas y comparamos con las vistas, parece haber cierta similitud. Entonces, al traer las filas de esta vista, también notamos cierto parecido en los nombres. Sin dudas, SCCM hace referencia a estas vistas para realizar las consultas desde su consola principal. Están todas las columnas pedidas, pero levemente modificadas. Entonces, si pasamos la consulta anterior a SQL con las modificaciones, nos quedaría de la siguiente forma:

```
select
SMS_R_SYSTEM.ResourceID,
SMS_R_SYSTEM.ResourceType,
SMS_R_SYSTEM.Name0,
SMS_R_SYSTEM.SMS_Unique_Identifier0,
SMS_R_SYSTEM.Resource_Domain_OR_Workgr0,
```

```
SMS_R_SYSTEM.Client0
from v_R_System as SMS_R_System
```

Vemos que a varias columnas se les agrega un número **0**, y las palabras del nombre son separadas por un signo _. De este modo, podemos llegar a fabricar nuestras propias consultas desde las herramientas de SQL. Otro ejemplo: si queremos traer todos los equipos que pertenezcan al site AD del país Argentina, agregamos el siguiente prefijo al final:

```
where SMS_R_System.AD_Site_Name0 = 'ARG'
```

Esta opción de poder analizar la base de datos y traer información que nos sea útil resulta de gran ayuda en investigaciones y pedidos de nuevos reportes. Sólo debemos analizar la definición de algún reporte ya creado que sea similar, y modificarlo con los parámetros adecuados.

... RESUMEN

Con lo visto a través de este capítulo podemos dar por terminado todo lo correspondiente a SCCM. Pudimos conocer la forma en que debemos realizar el manejo de la distribución, y el seguimiento de software y parches. También aprendimos a analizar reportes accediendo de todas las maneras posibles y a realizar colecciones de modo avanzado utilizando herramientas propias de MsSQL. En este capítulo tuvimos muchas secciones prácticas que nos facilitaron el aprendizaje de todas las configuraciones posibles de SCCM. Seguramente, encontraremos más, pero las más importantes fueron vistas en este libro.



ACTIVIDADES

TEST DE AUTOEVALUACIÓN

1 ¿Cómo se arma una colección estática?

2 Describa las diferencias entre colecciones estáticas y dinámicas.

3 ¿De qué forma distribuimos un paquete de software a los DPs?

4 ¿Cómo sabemos si el paquete de software se instaló correctamente en los DPs?

5 ¿En dónde realizamos las búsquedas de parches nuevos para distribuir por SCCM?

6 ¿Cómo armamos un paquete de actualizaciones nuevo?

7 ¿Cuál es la manera de hacer un seguimiento de la instalación de parches en la empresa?

8 ¿Cuántas formas de acceder a los reportes tenemos?

9 Enumere los reportes más importantes analizados en el libro.

10 ¿Cómo creamos una consulta avanzada en SCCM?

EJERCICIOS PRÁCTICOS

1 Cree varias colecciones intercalando colecciones dinámicas y estáticas.

2 Cree un instalador de software y realice un nuevo paquete de software para distribuir con SCCM.

3 Cree varias carpetas de búsqueda de actualizaciones con distintas opciones y genere una lista de parches.

4 Cree una colección de pruebas y distribuya la lista de actualizaciones anteriormente creada.

5 Cree un nuevo reporte a partir de una consulta avanzada utilizando el ayudante de SCCM para MS SQL.

Cómo expandir la tecnología de la empresa

Veremos a continuación algunos temas particulares que son muy importantes para expandir los límites de la tecnología implantada en nuestra empresa. Cloud computing es un concepto relevante, ya que implantar una configuración de nube en nuestra compañía nos hará crecer de manera significativa. También veremos algunas recomendaciones sobre investigación y expansión.

CONCEPTOS DE CLOUD COMPUTING

El cloud computing es uno de los temas más importantes al momento de publicar el presente libro. Muchas personas opinan sobre él, muchas conocen de esto, y otras no tanto, y nos hacen caer en confusiones. No es una nueva tecnología, como muchos piensan. El cloud computing es una forma de hacer negocios, de brindar un servicio a usuarios finales; es un modelo de consumo que desafía la aparición de nuevos métodos de cobro y de negocios en la empresa (intranet) y en la Red de redes (Internet). La tecnología que la sustenta es la virtualización.

Qué es cloud computing

Como dijimos, no se trata de una aplicación ni de una tecnología, sino que es una nueva forma de vender servicios IT en Internet, algo que existía antes en los negocios y que las empresas debían definir. La tecnología sobre la que se basan las soluciones de cloud computing es la virtualización, por sus características de poder brindar un tiempo cero de caídas de sistemas, y dar un servicio eficiente y robusto. Existen varias formas de vender servicios IT en Internet. Hay servicios de infraestructura que ofrecen servidores dedicados al usuario final, para que él pueda utilizarlo de manera remota, como si estuviera en una empresa. Este servicio se llama **IaaS** (*Infrastructure as a Service*), o infraestructura como servicio. También contamos con la opción de aplicaciones como servicios, llamada **SaaS**. En este caso, los empleados utilizan un software de terceros como si éste estuviese instalado en la compañía. El último servicio que podemos encontrar es **PaaS**, y se refiere a los servicios de desarrollo ofrecidos en Internet. Hace referencia a un servicio completo para desarrollo, que puede ser un lenguaje nuevo, un conjunto de servidores de bases de datos y desarrollo, etc. SaaS brinda servicios listos para consumir, en tanto que PaaS da un servicio para desarrollar aplicaciones utilizando las soluciones de terceros.
Resumiendo estos conceptos, tenemos IaaS, SaaS y PaaS. De ellos, el más renombrado en nuestro ámbito laboral de administración de servidores es PaaS, que tiene representantes liderando el mercado, como Google, con su servicio de **Google App Engine**; y Amazon, la pionera del cloud computing con su servicio **EC2**.



OPEN DATA CENTER ALLIANCE

Es una alianza de empresas que pretenden definir un estándar para la implementación del cómputo en la nube y nuevas tecnologías. Cada uno de los colaboradores se compromete a utilizar una guía estándar para la definición de sus ambientes. El comité está formado por líderes IT mundiales, como BMW, China Life, JPMorgan, Shell, Motorola, Nokia, Repsol YPF, Marriot, y otros.

***Figura 1.** En tan sólo tres pasos podemos empezar a construir nuestra primera aplicación en la nube.*

Ambos servicios cobran por transacciones hechas contra sus servidores en un determinado tiempo. El modelo de cobro es por consumo, al igual que para todos los servicios de cloud. El concepto de **se cobra lo que se usa** se aplica a todos los modelos de computación en la nube. En los servicios de SaaS podemos encontrarnos con empresas como **Salesforce**, que ofrece CRM en la nube. Esta firma cobra por el uso de su software online. También hay soluciones de antivirus o seguridad ofrecidas por **Symantec**, **McAfee** y varios competidores más. Por supuesto, ya conocemos las aplicaciones de correo electrónico, entre las cuales Google lidera el mercado con las soluciones gratuitas y comerciales de **Gmail**. Con respecto a IaaS, Microsoft ofrece **Azure**, a través de la cual entrega servidores de Exchange y de MsSQL, y cobra únicamente por su uso.

Las aplicaciones en la nube son el gran negocio presente y futuro, ya que permiten ofrecer cualquier tipo de software para el consumo masivo. La infraestructura en la nube ayuda a las empresas a pagar por lo que usan, sin tener que preocuparse por el mantenimiento que esto significa. Ya no hay que estar pendientes de actualizaciones, parches, caídas de servidores, cortes del servicio eléctrico, ni por generar un plan de respaldo ante desastres. Sin embargo, éste es un modelo un tanto preocupante para las grandes organizaciones que necesitan guardar su confidencialidad al extremo. Hoy en día, las áreas de IT dentro de las empresas son muy grandes, demandan cada vez más servidores, más especialistas y muchísimas más

conexiones entre los empleados para que el negocio avance. Cloud computing representa una solución para disminuir costos, pero poniendo en riesgo la seguridad y la confidencialidad de la compañía. Si todos optaran por el uso de cloud computing, muchos centros de cómputos dejarían de existir, aunque muchos otros crecerían enormemente. Tratemos de visualizar cómo sería el centro de cómputos de Google hoy en día, y cómo debería replicarse su infraestructura en varias ubicaciones geográficas para dar un servicio constante por más que hubiera un huracán. A pesar de que exista la virtualización y se haga extremo uso de ella, es preciso tener servidores físicos, que deben mantenerse en algún momento. Nuestro trabajo como administradores de servidores ya no será el mismo: está cambiando y tenemos que mirar hacia estas empresas que se comerán a los centros de datos de otras más pequeñas. Debemos especializarnos en virtualización y dar soluciones nunca antes imaginadas para llegar a liderar el mercado.

El cloud computing en la historia

Pensemos cómo llegamos al concepto de cloud. Tal vez al recordar de qué manera fue creciendo la informática a través de la historia, obtengamos una respuesta. Si miramos atrás en el tiempo, veremos que todo el cálculo de distintas empresas se agrupaba en los grandes mainframes en los años 60. Éstos eran gigantescas computadoras que ocupaban hasta manzanas enteras de extensión. Distintas empresas y usuarios finales alquilaban un tiempo o corrida del servidor para pasar sus tarjetas perforadas y, así, conseguir un resultado de los cálculos empleados en ciertas ecuaciones y estadísticas. Hasta que el mainframe no terminaba su trabajo y devolvía otras tarjetas perforadas, no había modo de saber si las entradas del análisis eran correctas. Demandaba mucha paciencia llegar a buenos resultados, porque se necesitaba el tiempo disponible de los mainframes, y en aquella época, éste escaseaba.
Luego aparecieron los monitores y los teclados, pero la descentralización del cómputo no desaparecía. Todo cambió cuando surgieron las computadoras personales, con un monitor y teclado propios. Estos equipos fueron una novedad y resultaban realmente costosos al principio. Pero entonces los usuarios ya no tuvieron que depender de los mainframes para realizar sus trabajos.



ENCLOSURE Y BLADES

Los enclosures son contenedores de servidores (blades) que comparten conectividad y alimentación. Se basan en una arquitectura hot plug (cambio de hardware en caliente) y en redundancia de cualquier tipo de elementos. Los blades son muy utilizados en virtualización y cloud computing por sus características de redundancia, ahorro de espacio y energía.

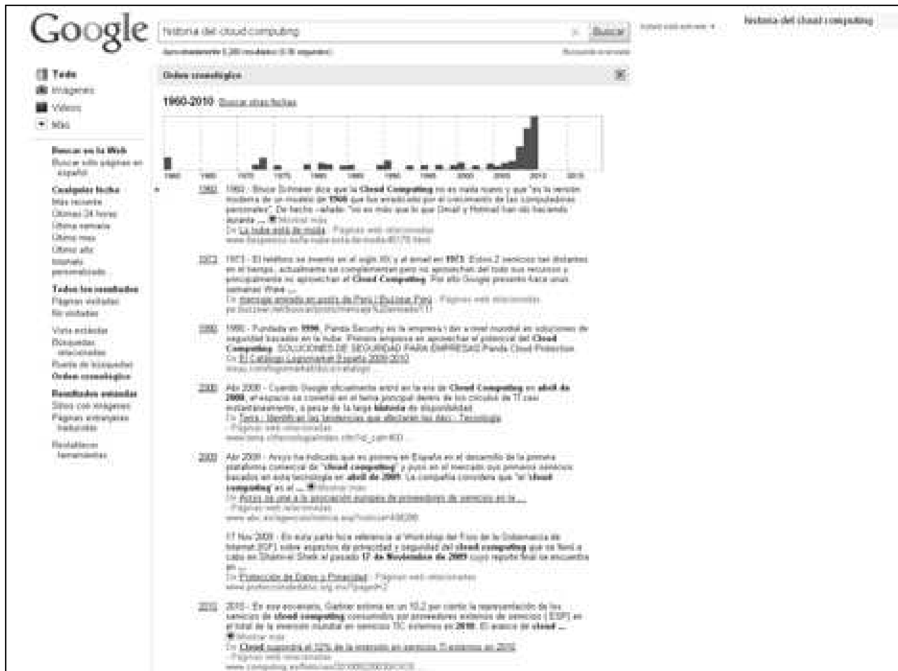


***Figura 2.** En los años 60, ya estaba formado el concepto de cloud computing, pero se dejó de lado para dar crecimiento a la computadora personal. En la imagen, una búsqueda cronológica de los conceptos.*

La computación personal se fue desarrollando de manera extraordinaria, y cada vez más y más empresas y familias tenían una PC. Se comenzó a evolucionar también en cuanto a tecnología de hardware, que fue creciendo y cambiando de forma exponencial. Cada vez era menor el tiempo que transcurría entre un cambio tecnológico y otro. Las notebooks y la movilidad se volvieron moda. Ya nada era novedad hasta que aparecieron las netbooks, los smartphones y las tabletas. Entonces nos pusimos un poco menos exigentes con las capacidades de las máquinas, para ganar en movilidad. Y fue así como estalló este nuevo concepto en todas partes. Los celulares se hicieron muy populares y avanzados: hoy tenemos en nuestras manos la capacidad de cómputo de 100 mainframes de los años 60. Se expandió la tecnología, y los conocimientos, las conexiones, la inteligencia humana y la capacidad de comunicarnos con el resto del mundo cambió radicalmente con Internet. Ahora, el concepto de los años 60 ya está pisando fuerte otra vez, al centralizar cómputo, economía, performance, seguridad, continuidad y escalabilidad.

Las redes sociales, como **Facebook** o **Twitter**, son servicios en la nube. Para el usuario común, dan la sensación de ser un solo sitio, pero atrás tienen todo el cómputo distribuido por todas partes del mundo. El usuario final no se da cuenta de cambios en parches o en hardware; sólo puede distinguir cambios en el software. La nube quizá nos sirva para evolucionar, ahora sí, en materia de aplicaciones, tema en el que

estamos un poco atrasados. La historia nos indica que avanzamos demasiado pronto en tecnología de hardware, sin que ocurriera lo mismo en materia de software. Había mucha capacidad de cómputo desperdiciada hasta la llegada de la virtualización. Podemos estar convencidos de que tratamos de utilizar todos los recursos disponibles de hardware con esta tecnología. Para que su uso sea óptimo, intentamos automatizar la construcción de nuevos recursos, de utilizar lo que realmente necesitamos, de darle agilidad a nuestro centro de cómputos con el uso de cloud computing. De esta forma, también optimizamos el tiempo de uso de los recursos para aprovecharlos al máximo.



***Figura 3.** El sistema operativo Android en los celulares se ha vuelto muy útil como entrada de datos para calcular el tráfico en las grandes ciudades, como Buenos Aires. Una vez más, Google aplicó una metodología de cloud.*

Todo el marco de cloud computing y virtualización nos da la puerta de entrada a un nuevo modo de pensar, de hacer software y trabajar en forma óptima.

Tipos de nubes

Cloud computing es una nueva forma de hacer negocios, de ofrecer servicios de IT por Internet y a través de una intranet (red interna de las empresas). Por eso existen tres tipos de nubes principales, además de los tres tipos de servicios que describimos anteriormente. Los ejemplos que dimos hasta ahora son de **nubes públicas**. Tanto Gmail como Hotmail tienen como cliente al público en general, que accede en forma masiva a consumir un servicio a través de Internet. Estos servicios siempre tendrán como cliente al público. El mismo concepto podría llevarse a la empresa internamente: cualquier departamento de IT podría ofrecer sus servicios en forma de cloud, automatizando totalmente el flujo de requerimientos y otorgamiento de recursos. Los otros departamentos podrían administrar fácilmente sus consumos, y podrían cobrarse los gastos mediante los presupuestos de distintas

áreas. Este tipo de nube es **privada**, porque está cerrada al total de las personas; el público ya no es el cliente, sino que lo es el empleado. La nube se expande hasta los límites de la organización. Un ejemplo es el correo electrónico: el empleado consume ese servicio pero no sabe realmente dónde está o cuán grande es, etc.
Luego, hay una conjunción de estas nubes, donde se mezclan las privadas y las públicas. Se las llama **mixtas o híbridas**, y un ejemplo puede ser un servicio que la empresa brinda al público y satisface también los requerimientos internos bajo el mismo sistema. Supongamos que Google no hace diferencia entre el uso interno o externo de Gmail: ésta sería una nube mixta. Los datos de los empleados internos y los del público en general se entremezclan en los mismos servidores y sistemas. En un ambiente de este tipo, se plantea la seguridad como aspecto principal para evolucionar. Los permisos a los servidores, usuarios administradores y permisos en carpetas se vuelven demasiado complejo de administrar. Éste es uno de los siguientes pasos en la evolución informática. En resumen, vimos los tres tipos de nubes que podemos llegar a encontrar: privadas, públicas y mixtas.

FUTURO DEL CLOUD COMPUTING

El cloud computing es un hecho: está entre nosotros y llegó para quedarse. Nadie sabe qué está tramando el destino para el sector IT, y quizá la respuesta esté en alguna película de ciencia ficción. Las grandes empresas ponen el foco en el cloud computing, y se están generando alianzas y organizaciones de numerosos participantes. También se están desarrollando diversas comunidades alrededor de las redes sociales y cadenas de usuarios. La administración de servidores está cambiando, y el cloud computing es el futuro.

Negocios actuales

En la actualidad, existen dos modelos de cobro con respecto al cloud computing: uno es el de uso gratuito, con el que se recauda dinero a través de las publicidades; el otro es el de cobro por el uso, donde los usuarios utilizan los recursos por los que pagan. Estos pagos pueden ajustarse dependiendo de la demanda, y existe una jerarquía de características que se van agregando dependiendo del plan de pagos. Este modelo es muy parecido al que antes usaban las empresas de hosting, donde había varios planes según las capacidades y existía una determinada cantidad de transacciones posibles en el período de cobro. Lo que realmente cambia en los negocios de cloud es el contrato SLA, con el cual la empresa que brinda el servicio da seguridad al usuario final. Dependiendo del monto del servicio, el contrato SLA puede ser más estricto o menos estricto; más caro o más económico.



***Figura 4.** Si accedemos al sitio oficial de SalesForce, tenemos la posibilidad de probar la solución de la nube durante un mes sin cargo, tan sólo con registrarnos como usuarios. El manejo es muy intuitivo y amigable.*

SalesForce cobra un monto por sus servicios, tiene varios planes y está creciendo de manera notable. Sus grandes competidores, como Siebel, Oracle o SAP, le están temiendo por su gran desarrollo en tan poco tiempo. La empresa fue fundada en 1999 por Marc Benioff, y hacia el año 2010 tenía más de 87.000 compañías como clientes, que manejan la información de sus empleados mediante su sistema cloud.
Google App Engine ofrece toda una plataforma de desarrollo para crear aplicaciones. Los costos de facturación van variando según el consumo y las conexiones a la aplicación creada. Si nuestra aplicación se hace popular y requiere más recursos, el costo del servicio aumentará. Sin embargo, hay un nivel que, a determinado límite de transacciones, se brinda de forma gratuita, y es para realizar pruebas y pequeñas aplicaciones. Otro servicio de Google que se puede ver como un SaaS es **Google Apps**. Se trata de un grupo de herramientas de oficina de acceso web. A diferencia de otros servicios, Google Apps cobra tan sólo 40 euros por usuario por año para todo tipo de usuarios.
Otro servicio, seguramente el más popular que podemos encontrar, es el de Amazon. Se denomina **Amazon Web Services** y tiene varios productos que ofrece en su sitio oficial; son muchos planes para todas las circunstancias que se nos puedan ocurrir.

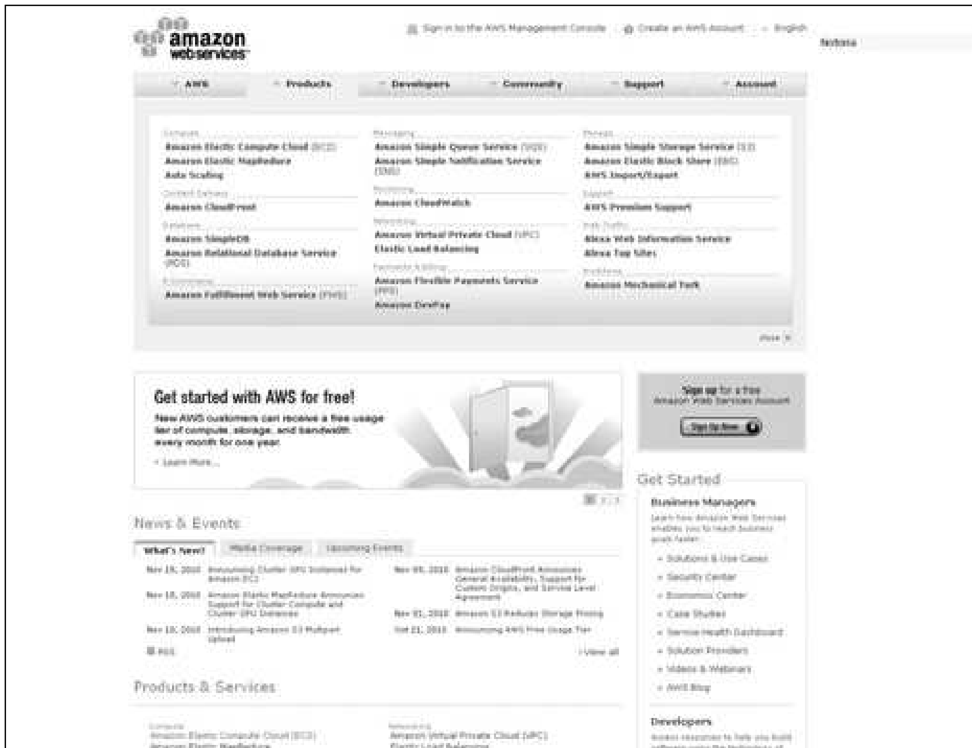


***Figura 5. Amazon Web Services** tiene 21 servicios posibles. Hay aplicaciones de cómputo en la nube, servicios de base de datos, e-commerce, mensajería, networking, monitoreo, almacenamiento, pagos, facturas y soporte técnico.*

Como existen numerosos planes, es muy engorroso calcular un costo. Para cada uno de estos servicios, hay unos cinco o seis tipos de precios según algunos límites, y a pesar de eso, las cifras cambian dependiendo de la localidad y el país en donde estemos. Sin dudas, Amazon tendrá que mejorar para ofrecer sólo un par de precios si quiere seguir creciendo. Fue la pionera en brindar este tipo de servicios, pero ha fragmentado mucho su negocio y deberá reacomodarse para seguir compitiendo.

Evolución y nuevos negocios

Sin dudas, la evolución en cloud computing estará en la mejora de seguridad. Esto hará que las grandes empresas del mundo necesiten contar con un servicio de cloud. Seguramente, habrá que buscar la manera de garantizar la seguridad. Hoy en día, los contratos de confidencialidad se hacen a un lado ante los requerimientos de pedidos gubernamentales. Esto es un riesgo, ya que nadie sabe qué se está pidiendo, qué se está dando, y nadie calcula los peligros y los trastornos que esto puede ocasionar hoy a una gran empresa. Ya ocurrió con el servicio de Gmail, en el cual el gobierno hizo intervenir ciertas cuentas de correo electrónico.

Seguramente, también se requiera alguna otra forma de administración de cuentas, y que se pueda administrar una sola cuenta entre varios servicios de cloud. Si por cada servicio, cada aplicación, tendremos un perfil, estadísticas y gastos, necesitaremos administrarlos todos juntos. Se plantean grandes desafíos por delante para seguir creciendo tecnológicamente, y la continuidad del negocio dependerá de nosotros, pero según la empresa en la que trabajemos. El futuro del cloud computing es prometedor, aunque también esgrime peligros y desafíos. Los datos como información pueden ser los detonadores del mañana. Al respecto, gran lección nos dio Wikileaks. Nadie está exento de la verdad. A continuación, veremos un tema importante en la expansión de la tecnología: la virtualización de escritorios.

VIRTUALIZACIÓN DE ESCRITORIOS

Más allá de los servidores, también existen varias soluciones para virtualizar todas las máquinas de escritorio de la empresa. Virtualizar una PC es lo mismo que hacerlo con un servidor, pero implica otros desafíos masivos, porque hay que cambiar el accionar de muchas personas al mismo tiempo. A continuación, haremos una introducción a estos conceptos, veremos las soluciones de VMware y, luego, analizaremos aplicaciones virtuales con Citrix. Por último, mostraremos hasta dónde llega hoy la virtualización de escritorios.

Introducción a la virtualización de escritorios

Todo comenzó con el descubrimiento de la virtualización en plataformas x86 alrededor de los años 90. En un primer paso, los empleados seguían trabajando con sus laptops y máquinas de escritorio, pero utilizaban un equipo virtual alojado en un servidor central en el datacenter. Con el correr de los años, comenzaron a usarse terminales, también llamadas clientes ligeros. Estos equipos eran parecidos a las máquinas de escritorio, pero se basaban en un mínimo hardware, dispositivos de entrada/salida y un monitor. La terminal se conectaba directamente al servidor de virtualización para traer la máquina virtual correspondiente hasta el usuario. Éste era reconocido por la terminal mediante una tarjeta magnética que debía llevar a cualquier lugar de la empresa en donde quisiera usar su entorno de trabajo. De esta manera, los administradores podían mantener centralizados todos los datos de la compañía y, también, tener una configuración estándar para todas las máquinas, de forma muy ágil y sin gastar demasiados recursos. Esta modalidad también reducía enormemente los gastos de hardware y el consumo de energía, y aumentaba la continuidad del negocio, ya que los entornos de los empleados siempre estaban vivos en el servidor de virtualización.



Figura 6. *La virtualización de escritorios se viene utilizando desde hace años. Brinda una gran flexibilidad a la hora del testing y el desarrollo de sistemas.*

La virtualización de escritorios es un poco compleja porque plantea una pérdida de autonomía y privacidad para el usuario final. En una empresa seria, esto no ocasiona conflictos porque los activos son de ella, no de los empleados; y deben utilizarse para el trabajo diario y nada más. Para estos casos, existen varias soluciones en el mercado. Microsoft cuenta con **Microsoft Enterprise Desktop Virtualization**; en tanto que VMware ofrece **VMware View**, que tiene un gran rango de compatibilidad con los clientes ligeros del mercado. También hay herramientas de SUN y Citrix muy ligeras y parecidas a las anteriores.

Herramientas para la virtualización de aplicaciones

Con el advenimiento de la virtualización de los escritorios, faltaba algo que centralizara la administración de las aplicaciones, que facilitara la administración y centralizara las aplicaciones corporativas. La solución se basó en un concepto antes usado por empresas como Microsoft, con sistemas de Terminal Servers (terminales de servicio). Los usuarios accedían a las terminales de servicio a través del acceso remoto y veían un menú con las aplicaciones corporativas que podían utilizar. Hoy en día, las soluciones dan al usuario una experiencia mucho más cercana a la real,

como si tuviesen las aplicaciones instaladas localmente. Microsoft desarrolló una solución híbrida con su sistema operativo **Windows 2008**, donde mezcló el servicio de terminales con aplicaciones virtualizadas. VMware también cuenta con una herramienta para este fin, llamada **ThinApp**, pero sin dudas, la que maneja el mercado es Citrix, con su producto **XenDesktop**. Esta solución va más allá y ofrece las aplicaciones en cualquier dispositivo, ya sea desktop, laptop o teléfonos móviles. Con sólo tener un navegador, ya se puede disfrutar de cualquier aplicación corporativa.

Google y la virtualización de escritorios

A fines del año 2010, Google presentó su nuevo sistema operativo **Google Chrome OS**, que más que eso, es una notebook con sistema operativo, toda una solución de escritorio. Contiene un cliente ligero, ofrecido en forma gratuita, que centraliza los escritorios en sus datacenters. Google se basó en la seguridad, en la simplicidad y en la velocidad para ofrecernos la mejor experiencia. Al encender la notebook, se inicia un minisistema operativo y, luego, se conecta a Internet para presentarnos nuestro escritorio. Si la notebook no tiene conexión, trabaja con una caché local que permite seguir utilizando el escritorio. Todos nuestros datos están encriptados gracias a un firmware incorporado en el dispositivo. Éste se asocia con nuestra clave para que nadie más que nosotros pueda acceder a la información, con lo cual nuestros datos quedan completamente asegurados. Nuestro escritorio así presentado es muy simple y fácil de usar. Si cambiamos de dispositivo, lo conservaremos tal como lo dejamos, porque se encuentra en Internet. El sistema operativo siempre tiene la última versión disponible, sin nuestra intervención, lo que brinda la máxima seguridad lo más rápido posible. Desde una conexión a Internet, podemos instalar aplicaciones muy fácilmente yendo a la tienda de Google, donde hay numerosas alternativas gratuitas y pagas.

Este escritorio virtual fue desarrollado por Google, más que nada, para uso empresarial. También puede usarse en el hogar, pero su seguridad extraordinaria lo hace perfecto para que las compañías dejen de lado sus máquinas antiguas, con problemas de hardware y de software. El Helpdesk se reduce mucho, porque si una de estas notebooks falla, Google la cambia por otro equipo.

GOOGLE - CHINA

El gobierno de China invadió cuentas de Gmail de defensores de los derechos humanos. Fue una investigación interna de Google la que estableció estos resultados, y hasta puso en peligro las relaciones internacionales entre EE.UU. y China. Veinte compañías se sumaron a este ataque desde esta última nación. ¿La tercera guerra será vía Internet?

Una opción muy adecuada para las empresas viene de la mano de Citrix y se llama **Citrix Receiver**. Con esta solución, las empresas pueden ofrecer sus aplicaciones corporativas a los empleados, estén donde estén, a través de Internet. El usuario coloca sus credenciales y aparece un menú con todas las aplicaciones que puede instalar en el escritorio: un administrador de planillas de cálculo Excel, un cliente SAP o algún otro servicio que no necesariamente tenga una versión web. Es importante mencionar que una vez hecho esto, tendrá fácil acceso desde su escritorio, como con cualquier otra aplicación propia de Google.



Figura 7. *La laptop que usará Google para brindar su sistema operativo embebido no tiene grandes características: es muy simple y no posee tecla TAB. En su lugar, tiene una lupa.*



APLICACIONES QUE OFRECE GOOGLE APPS

Google Apps es pago. Ofrece 25 GB por cuenta del servicio de Gmail, correo online las 24 horas, Calendar, el mismo calendario en todas partes, y grupos de Google. Es muy utilizado por las pymes por su bajo costo y sus posibilidades de crecimiento, pero no así por las grandes corporaciones, debido a conflictos de seguridad.

Su alta seguridad, nulo soporte técnico, velocidad y bajo costo hacen de este tipo de escritorios un producto incomparable. Su primera salida al mercado fue un proyecto beta en el cual participaron varias empresas importantes de los Estados Unidos de forma anónima y por decisión propia. La empresa Google entregó miles de máquinas. En este sentido, se espera que el equipo que brinda la máquina virtual sea lanzado al mercado en el transcurso del año 2011.

INVESTIGACIÓN EN IT

Debemos tener en cuenta que la investigación se convierte en una tarea diaria para el administrador de sistemas; siempre hay que resolver problemas de todo tipo. Es muy importante saber investigar bien, dónde buscar y utilizar las herramientas que tenemos para no fallar. A continuación, veamos algunos consejos.

Cuándo, cómo y dónde investigar

Es necesario saber cuándo, cómo y dónde investigar para acelerar nuestra administración. Varias veces nos plantearemos estas dudas. Si queremos saber cuándo vamos a investigar, la respuesta es siempre: ya sea por un problema específico que se plantee o para actualizarnos sobre alguna tecnología.

Un problema puede ser alguna falla en nuestros equipos o, también, algo que necesitamos hacer y no sabemos cómo lograrlo. Si pensamos **cómo** deberíamos hacerlo, tendríamos que establecer pasos distintos en estos dos tipos de investigaciones. En caso de que ocurra un problema, tendremos que usar algún método de **troubleshooting** (sistemas universales para la solución de inconvenientes). Algunos pasos para seguir son:

- Prepararse
- Hacer un control de daños
- Conseguir la descripción completa y exacta del síntoma
- Reproducir el síntoma
- Hacer el mantenimiento correctivo
- Afinar la búsqueda de la causa raíz
- Arreglar o reemplazar el componente dañado
- Probar
- Enorgullecerse
- Evitar futuras ocurrencias

Es interesante mencionar que es posible modificar estos pasos o crear los propios, pero básicamente son los que se encuentran mencionados en la lista.

Ahora, si pensamos en el **dónde**, cualquier investigación que realicemos se basará en el uso de Internet como fuente principal y también en libros si el tema es muy específico. En cualquiera de los dos casos, necesitamos confirmar la confiabilidad de la información, la experiencia y la trayectoria de quien escribe. Ambos mundos son inmensos hoy en día, y cualquiera puede escribir, pero no todo tiene la misma calidad. Lo recomendable es, en primer lugar, buscar información en sitios oficiales y, luego, avanzar a otras fuentes. Si estamos investigando tecnología nueva, debemos buscar en presentaciones oficiales de la compañía propietaria del desarrollo, en revisiones de expertos, en las notas y en foros donde es posible leer opiniones sobre los productos. Todo esto nos permitirá sacar nuestras propias conclusiones para crear las mejores soluciones posibles.

Lugares y sitios recomendados

Al tener un problema, quizá sea más aconsejable preguntar a algún colega que sea experto en el tema, antes que investigar por nuestra cuenta. Tener una gran cartera de colegas a mano es imprescindible para el administrador. Necesitamos contar con nuestras redes profesionales como primer punto de partida. Un buen sitio para crear redes es **LinkedIn**; aunque haya otras opciones, ésta es la más grande al día de hoy. Un punto interesante es hacernos socios de sitios de expertos, redes sociales profesionales y de temas específicos, para encontrar rápidamente a alguien que pueda ayudarnos ante un problema. Entonces, como dijimos antes, Internet es la principal fuente, pero dentro de ella, debemos hacernos un camino. Por ejemplo, en **Technorati** hay numerosos blogs, pero presentados en orden de importancia, con votos de la gente que los lee. Los que estén en la cima serán los mejores. Éste es un buen punto de partida.
También podemos investigar en los **sitios y blogs de los creadores** de los sistemas. Por ejemplo, si buscamos una solución a un problema de System Center, podríamos investigar en el blog de sus creadores; hasta tal vez podríamos escribir una consulta por e-mail a alguno de ellos o al equipo. Antes, era impensable **hablar con el autor de un libro** o manual, o con alguien que hubiera desarrollado una tecnología, pero hoy contamos con el correo electrónico y con las redes, que nos acercan sin importar las distancias físicas ni las diferencias de idiomas.



BUSCADORES

Google es el rey de los buscadores, pero no toda la información del mundo está allí. Hay mucha que aparece en otros buscadores. Existen numerosos laboratorios, centros de investigación y empresas que no permiten la entrada de buscadores para indizar su información. Por eso, es conveniente utilizar otras fuentes de datos como ayuda para nuestras investigaciones.

Recomendaciones de un estudiante de ingeniería

En primer lugar, debemos analizar el tamaño del problema, ver en dónde y cómo incide, en qué sistemas, en qué departamentos, a cuántas personas afecta y cuántos gastos podemos provocar en caso de que haya un fallo. Tener un panorama amplio, y no sólo del problema puntual, nos ahorrará muchos dolores de cabeza y, también, pérdidas económicas. Esto nos dará cierta tranquilidad en el trabajo.

Casi siempre ocurrirá que necesitemos hacer algo que ya hicimos antes. Muchas veces tenemos que investigar a contra tiempo y resolver las situaciones con rapidez. Lo mejor es tener nuestra propia base de conocimientos, y hacer un blog con estas investigaciones, soluciones propias analizadas y desmenuzadas por nosotros mismos. También podríamos compartir este blog con la comunidad, por si alguien tiene el mismo problema, o sólo tenerlo en privado para consultar antes que cualquier otra alternativa. Al afrontar un problema, es importante entender qué queremos resolver. No sólo debemos llevar a cabo acciones que estén en un paso a paso, sino que precisamos entender bien el funcionamiento completo. Cuando hagamos el análisis de incidencias, deberemos hacerlo desde el punto de vista informático y, también, desde el humano. Las personas se acostumbran a utilizar ciertos sistemas, a realizar acciones de una forma determinada, y si cambiamos eso, puede resultar catastrófico. Si entrevistamos a los usuarios, podríamos descubrir aspectos impensables, considerando la postura de alguien que no tiene nuestros conocimientos.

... RESUMEN

Hemos visto en este apéndice muchos de los temas actuales del sector IT. Estas tecnologías están en auge y en pleno desarrollo. Nos hemos sumergido en el mundo del cloud computing, analizando el concepto a través de la historia y del negocio en sí. También describimos algunas características que hacen de la virtualización de escritorios una herramienta poderosa. Sin dudas, investigar no es nada fácil, pero también aprendimos algunos conceptos que nos ayudarán con nuestro trabajo diario y arduo de mantener la continuidad del negocio en pie.

Servicios al lector

En el último apartado de este libro encontraremos un índice temático con las palabras más significativas que están presentes en esta obra. Además, una guía que nos servirá para conocer sitios web con información relacionada.

ÍNDICE TEMÁTICO





SITIOS WEB RECOMENDADOS

VMware

www.vmware.com

VMware es una de las herramientas de virtualización que hay en el mercado, precursora en tecnología x86 y x64. Es la empresa que maneja el camino en la virtualización de servidores. Encontramos todo tipo de software y documentación.



SCCM

www.microsoft.com/systemcenter/en/us/configuration-manager.aspx

Es el sitio oficial de System Center Configuration Manager, una de las herramientas en las cuales se centra el libro y esencial para la administración. Incluye todos los detalles, documentación, laboratorios y versiones beta de la herramienta.



Microsoft Research

http://research.microsoft.com

Es la web de los laboratorios de investigación de Microsoft. Allí se publican artículos técnicos, noticias, eventos y software en desarrollo para la comunidad. Es un buen sitio para descubrir la tecnología que viene y probar las versiones beta de los programas a instalar en nuestra empresa para saber las repercusiones.



Google Labs

www.googlelabs.com

Se trata del sitio web donde Google se encarga de publicar sus nuevas ideas, sus nuevos proyectos, con datos interesantes para los usuarios finales. Podemos encontrar miles de aplicaciones listas para probar e involucrarse en los procesos de desarrollo correspondientes y, de esta forma, ayudar a la comunidad.



Yahoo Labs

http://labs.yahoo.com

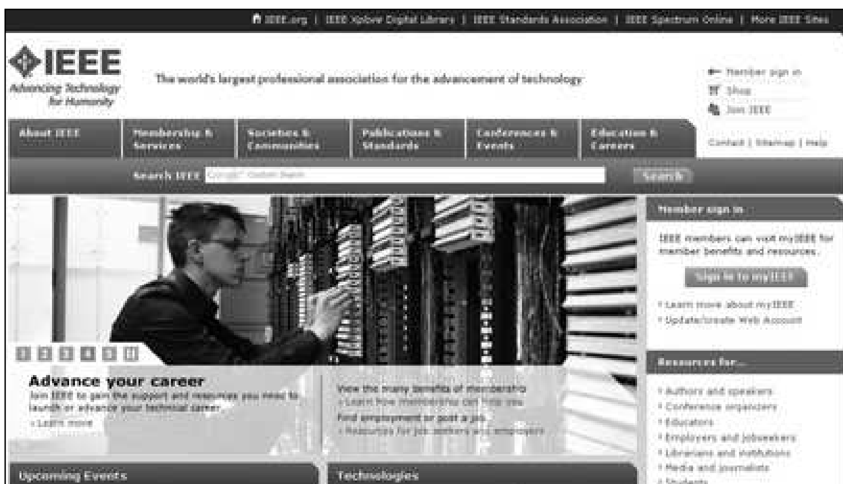
En esta dirección podemos encontrar el más extraordinario sitio de investigación de la importante empresa Yahoo. A medida que naveguemos por sus páginas, nos daremos cuenta de que posee un contenido muy ordenado, gran diseño en su sitio, publicaciones, laboratorios, noticias, eventos, etc.



IEEE

www.ieee.org

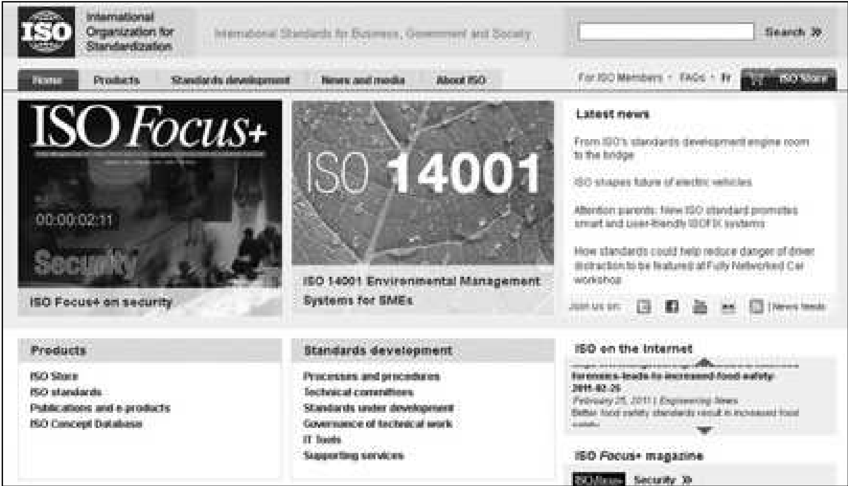
Se trata de la institución técnica más grande del mundo, que agrupa a los ingenieros en electricidad y electrónica. En el sitio web es posible encontrar todos los papers publicados, todos los estándares creados, además de conferencias, una sección de membrecía muy importante, una librería, etc.



ISO

www.iso.org

El sitio oficial de la organización internacional de estandarización. Se trata del organismo que se preocupa de definir los estándares del mundo en distintas materias. Hay muchas normativas de sistemas, como la ISO9001, la ISO27000 de seguridad, etc. Podemos encontrar gran cantidad de información.



ITIL

www.itil.org

El sitio oficial de las normas ITIL. Se trata de normas de sistemas que se aplican en todas las empresas. En el último tiempo han cobrado gran importancia sin llegar a ser normativas internacionales, pero con todos los motivos para serlo. Posee una gran cantidad de información y todos los pasos a seguir.



Symantec

www.symantec.com/es

Es el sitio inicial de la empresa Symantec. En esta web podemos encontrar una gran cantidad de información sobre sus productos, avisos de vulnerabilidades y varios datos relevantes relacionados con la seguridad de nuestros equipos; además, incorpora importantes noticias sobre cloud computing.



Trend

http://es.trendmicro.com

Se trata del sitio oficial de la empresa Trend. Aquí podemos acceder y obtener información relevante sobre todos los productos ofrecidos por la compañía; también encontraremos alertas sobre posibles vulnerabilidades y notas de seguridad relacionadas con la protección de nuestra información.



McAfee

www.mcafee.com/es

Otra de las empresas de seguridad. Se presenta como una de las grandes compañías relacionadas con la protección y la seguridad informática. En el sitio podemos ver las soluciones ofrecidas para organizaciones y para el público en general. Por supuesto, también encontraremos notas de seguridad, soporte, etc.



Microsoft Security Advisories

www.microsoft.com/technet/security/advisory

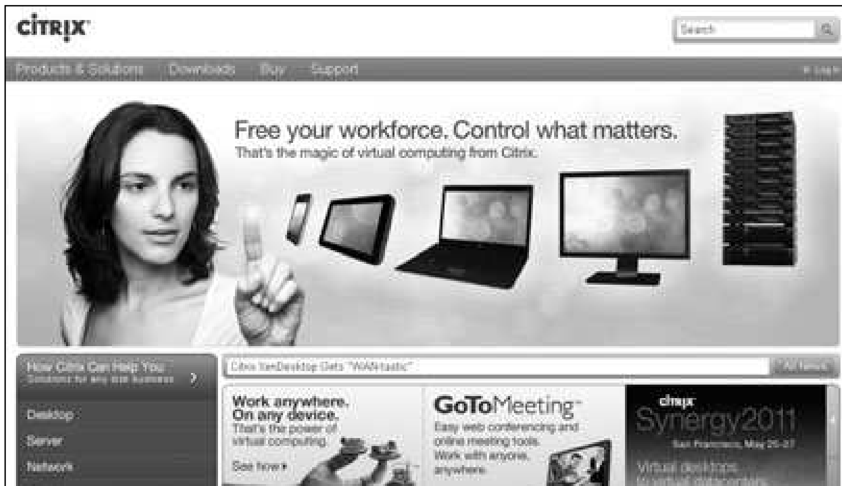
En este sitio de Microsoft se publican todos los boletines de seguridad en los cuales se detallan las nuevas vulnerabilidades encontradas junto a sus soluciones. Es un buen comienzo en el análisis de la instalación de parches y, por lo tanto, un sitio que debemos tener en cuenta para administrar sistemas informáticos.



Citrix

www.citrix.com

Página oficial de Citrix, una empresa de virtualización orientada a la implementación de esta tecnología en desktops, pero que también ofrece herramientas de este tipo para servidores y aplicaciones virtuales diversas. Entre sus páginas encontraremos información y datos relacionados con la virtualización en general.



El Blog de la virtualización

www.josemariagonzalez.es

Este blog se especializa en virtualización. Posee una gran cantidad de colaboradores especialistas en seguridad informática, los cuales comparten sus notas con el mundo. Si accedemos al contenido ofrecido, podemos aprender mucho con notas técnicas de todo tipo y videotutoriales extraordinarios.



Hispavirt

https://hispavirt.wordpress.com

Hispavirt es un blog de virtualización en castellano; se trata de uno de los que ofrecen el más alto nivel técnico en las notas publicadas. Podremos darnos cuenta de que está muy bien categorizado, y si queremos hacer alguna configuración compleja, éste es el mejor lugar donde buscar la ayuda que necesitamos.



Ingeniería en sistemas

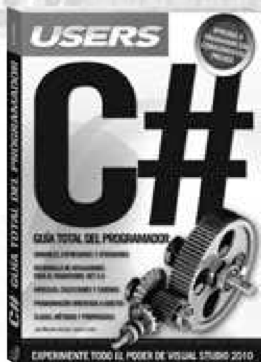
www.infosobresistemas.blogspot.com

Es el blog del autor de este libro, en donde es posible encontrar información de sistemas y nuevas tecnologías, así como también notas técnicas sobre virtualización, cloud computing y SCCM, entre otras. Ofrece un nivel técnico especializado, por lo que se trata de una ayuda imprescindible para los usuarios.



¡Léalo antes Gratis!

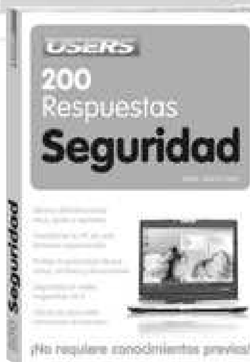
En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



C#

Este libro es un completo curso de programación con C# actualizado a la versión 4.0. Ideal tanto para quienes desean migrar a este potente lenguaje, como para quienes quieran aprender a programar desde cero en Visual Studio 2010.

→ COLECCIÓN: MANUALES USERS
→ 400 páginas / ISBN 978-987-26013-5-5



200 Respuestas Seguridad

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos contestar para conseguir un equipo seguro. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-26013-1-7



Funciones en Excel

Este libro es una guía práctica de uso y aplicación de todas las funciones de la planilla de cálculo de Microsoft. Desde las funciones de siempre hasta las más complejas, todas presentadas a través de ejemplos prácticos y reales.

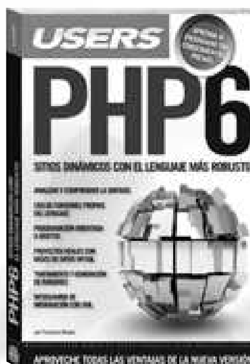
→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-26013-0-0



Proyectos con Windows 7

En esta obra aprenderemos cómo aprovechar al máximo todas las ventajas que ofrece la PC. Desde cómo participar en las redes sociales hasta las formas de montar una oficina virtual, todo presentado en 120 proyectos únicos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-036-8



PHP 6

Este libro es un completo curso de programación en PHP en su versión 6.0. Un lenguaje que se destaca tanto por su versatilidad como por el respaldo de una amplia comunidad de desarrolladores, que lo convierten en un punto de partida ideal para quienes comienzan a programar.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-039-9



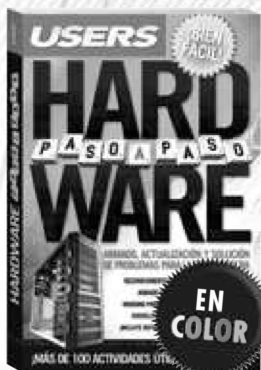
200 Respuestas: Blogs

Esta obra es una completa guía que responde a las preguntas más frecuentes de la gente sobre la forma de publicación más poderosa de la Web 2.0. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-663-037-5



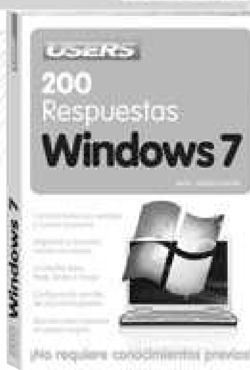
usershop.redusers.com



Hardware paso a paso

En este libro encontraremos una increíble selección de actividades que abarcan todos los aspectos del hardware. Desde la actualización de la PC hasta el overclocking de sus componentes, todo en una presentación nunca antes vista, realizada íntegramente con procedimientos paso a paso.

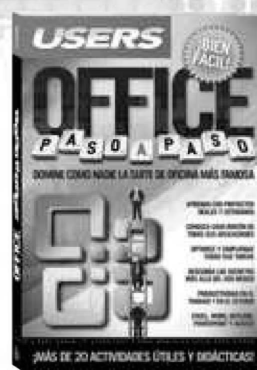
→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-034-4



200 Respuestas: Windows 7

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos conocer para dominar la última versión del sistema operativo de Microsoft. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-663-035-1



Office paso a paso

Este libro presenta una increíble colección de proyectos basados en la suite de oficina más usada en el mundo. Todas las actividades son desarrolladas con procedimientos paso a paso de una manera didáctica y fácil de comprender.

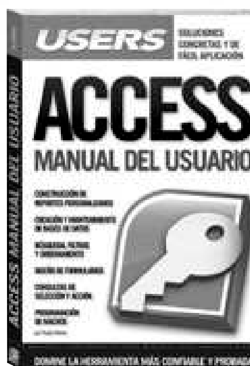
→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-030-6



101 Secretos de Hardware

Esta obra es la mejor guía visual y práctica sobre hardware del momento. En su interior encontraremos los consejos de los expertos sobre las nuevas tecnologías, las soluciones a los problemas más frecuentes, cómo hacer overclocking, modding, y muchos más trucos y secretos.

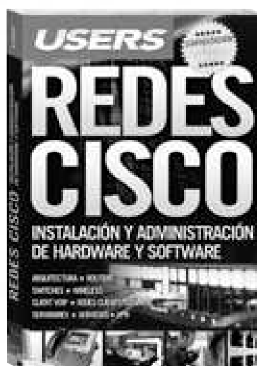
→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-029-0



Access

Este manual nos introduce de lleno en el mundo de Access para aprender a crear y administrar bases de datos de forma profesional. Todos los secretos de una de las principales aplicaciones de Office, explicados de forma didáctica y sencilla.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-025-2



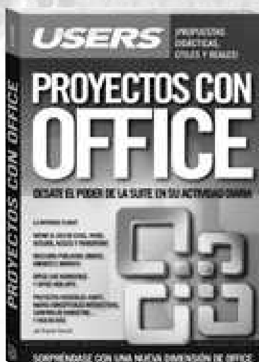
Redes Cisco

Este libro permitirá al lector adquirir todos los conocimientos necesarios para planificar, instalar y administrar redes de computadoras. Todas las tecnologías y servicios Cisco, desarrollados de manera visual y práctica en una obra única.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-024-5

¡Léalo antes Gratis!

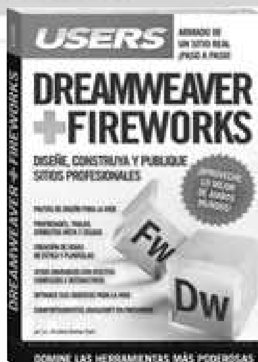
En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Proyectos con Office

Esta obra nos enseña a usar las principales herramientas de Office a través de proyectos didácticos y útiles. En cada capítulo encontraremos la mejor manera de llevar adelante todas las actividades del hogar, la escuela y el trabajo.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-023-8



Dreamweaver y Fireworks

Esta obra nos presenta las dos herramientas más poderosas para la creación de sitios web profesionales de la actualidad. A través de procedimientos paso a paso, nos muestra cómo armar un sitio real con Dreamweaver y Fireworks sin necesidad de conocimientos previos.

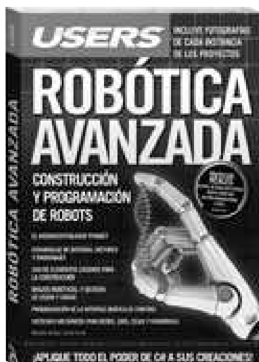
→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-022-1



Excel revelado

Este manual contiene una selección de más de 150 consultas de usuarios de Excel y todas las respuestas de Claudio Sánchez, un reconocido experto en la famosa planilla de cálculo. Todos los problemas encuentran su solución en esta obra imperdible.

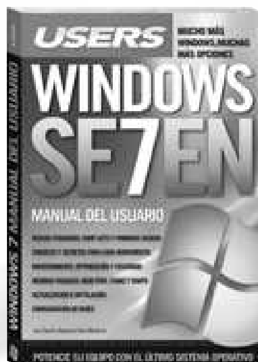
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-021-4



Robótica avanzada

Esta obra nos permitirá ingresar al fascinante mundo de la robótica. Desde el ensamblaje de las partes hasta su puesta en marcha, todo el proceso está expuesto de forma didáctica y sencilla para así crear nuestros propios robots avanzados.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-020-7



Windows 7

En este libro, encontraremos las claves y los secretos destinados a optimizar el uso de nuestra PC tanto en el trabajo como en el hogar. Aprenderemos a llevar adelante una instalación exitosa y a utilizar todas las nuevas herramientas que incluye esta versión.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-015-3



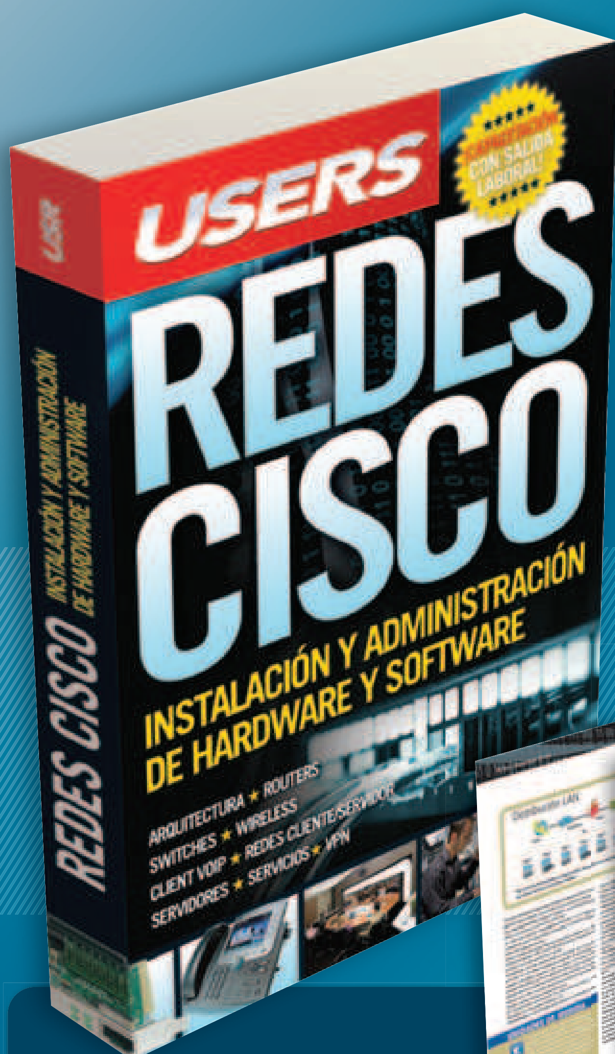
De Windows a Linux

Esta obra nos introduce en el apasionante mundo del software libre a través de una completa guía de migración, que parte desde el sistema operativo más conocido: Windows. Aprenderemos cómo realizar gratuitamente aquellas tareas que antes hacíamos con software pago.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-013-9

usershop@redusers.com

PLANIFICACIÓN, INSTALACIÓN Y ADMINISTRACIÓN DE REDES COMPLEJAS



Este libro permitirá al lector adquirir todos los conocimientos necesarios para planificar, instalar y administrar redes de computadoras. Todas las tecnologías y servicios Cisco desarrollados de manera visual y práctica en una obra única.

- REDES / EMPRESAS
- 320 PÁGINAS
- ISBN 978-987-663-024-5





USERS

CONTENIDO

1 | ADMINISTRACIÓN INTERNA DE UNA EMPRESA
Infraestructura de una empresa / Tipos de redes / Equipamiento de una red / Herramientas necesarias para un administrador / Servidores corporativos / Servicios necesarios en una empresa

2 | CONFIGURACIONES DEL SERVIDOR
Instalación / Seguridad básica / Configuraciones básicas / Importancia del correo / Aplicaciones de seguridad / Herramientas / Accesos remotos / Paneles de control / Informes

3 | SEGURIDAD CORPORATIVA
Políticas de seguridad / Plan de contingencias / ITIL y la norma ISO20000 / Antivirus y firewalls / Definición de reglas de seguridad

4 | VIRTUALIZACIÓN DE SERVIDORES
Qué es la virtualización / VMware / Cómo instalar ESX y ESXi / Cómo crear una máquina virtual / Cómo virtualizar un servidor / Virtual Center / Virtual Appliance

5 | ADMINISTRAR VMWARE VSPHERE
Qué es vSphere y cómo instalarlo / Herramientas de vSphere / Qué es Vmotion / Detalles del sistema DRS / Conceptos de Fault Tolerance / Herramientas de actualización / Backups de ambientes VMware / Snapshot / Soluciones de Backup

6 | SYSTEM CENTER CONFIGURATION MANAGER
Microsoft System Center / Instalación de SCCM / Roles de servidores / Clientes de SCCM / Consola de comprobación de clientes / Mejoras utilizando P2P

7 | PROGRAMAS, PARCHES E INFORMACIÓN
Colecciones estáticas y dinámicas / Paquetes de software / Distribuciones / Creación de parches / Análisis y seguimiento de parches / Reportes / Base de datos de SCCM

APÉNDICE | EXPANDIR LA TECNOLOGÍA DE LA EMPRESA
Cloud computing / Negocios actuales / Evolución y nuevos negocios / Virtualización de escritorios / Google y la virtualización / Investigación en IT / Cuándo, cómo y dónde investigar

NIVEL DE USUARIO

PRINCIPIANTE | INTERMEDIO | AVANZADO | EXPERTO

ADMINISTRADOR DE SERVIDORES

Este libro es la puerta de acceso para ingresar en el apasionante mundo de los servidores; de gran utilidad para quienes se desempeñan como soporte de escritorio y quieren comenzar a trabajar como administradores, así como también para estudiantes, gerentes de IT y aquellos que trabajan en áreas relacionadas. Al comenzar su lectura, aprenderemos los conocimientos básicos necesarios sobre hardware y redes, para luego adentrarnos en la instalación y configuración, reglas y normas de seguridad. Luego, nos ocuparemos de dos herramientas muy importantes para la virtualización de servidores y su administración: VMware y System Center Configuration Manager. Repasaremos las características principales y la instalación de estas dos soluciones, además de dar un vistazo a su futuro. Al finalizar el libro, contaremos con todas las herramientas y los conceptos requeridos para ser administradores de servidores ágiles y eficientes, de modo de tener el control de todos los servidores en la palma de nuestra mano.



RedUSERS.com

En este sitio encontrará una gran variedad de recursos y software relacionado, que le servirán como complemento al contenido del libro. Además, tendrá la posibilidad de estar en contacto con los editores, y de participar del foro de lectores, en donde podrá intercambiar opiniones y experiencias.

Si desea más información sobre el libro puede comunicarse con nuestro Servicio de Atención al Lector: usershop@redusers.com

SERVER ADMINISTRATOR



This book is the access gateway to the fascinating server administration world. It covers concepts such as virtualization, corporate security rules and policies, monitoring and reporting, as well as costs reduction and cloud computing, among others.


ISBN 978-987-1773-19-0





